代　序

华罗庚教授的《数论导引》是写得很好的一部专著，而任承俊同志编写的这本《数论导引提要及习题解答》，对于学习《数论导引》的人将会很有帮助。不过，读者在做题时，首先还是应当独立思考、刻苦钻研，得出结果后再翻阅题解；只当确感困难时，才求助于本书。这样，则既可锻炼提高自己的解题能力，又不至于在障碍面前束手无策。

书此数语，不知读者以为然否？

柯　召

1985年5月

前　言

随着科学技术的不断发展，数论这一“古老”而又“年轻”的学科，在技术领域中得到了许多卓有成效的应用．这引起了人们对数论的瞩目，同时也激发了广大青少年的兴趣．要求学习、掌握数论知识的人越来越多了．

华罗庚教授所著《数论导引》是数论书籍中的一部名著．该书从一九五七年问世到一九七九年已经五次印刷，但是迄今国内还未曾出版过与之相配合的习题解答．而华先生在介绍维诺格拉托夫的《数论基础》时就曾说过：“如果读这本书而不看不做书后的习题，就好象入宝山而空返，把这书的最重要的部分忽略了！”可见，要学习好数论，必须做大量的习题．本着为学习数论的同志提供解题参考的目的，我不揣浅陋，编写了这本《数论导引提要及习题解答》．

本书各章均由提要和习题解答两部分组成，前者列出了相应于各章的定义、定理，而后者则给出了全部习题的解答．此外，还有对于习题及答案中一些疏漏的订正，以及对某些有关问题的介绍和讨论等．全书共二十章．原书部分章节无习题（如第十八章，第一章中的§2、§3、§4等），本书将这些章节略去了．但目录中仍列出了第十八章的章名．

应当着重指出的是，在编写本书初稿的过程中，我始终得到了著名数学家柯召教授的关怀与鼓励．脱稿后，柯老又在百忙中对全书进行了审阅，且为一些难度较大的题目提供了解题思路，

或亲自给予了详细解答。就是说，本书凝结着老一辈科学家的心血，体现了老一辈科学家的人梯精神。

尽管有柯老指教，但限于本人水平，本书仍难免疏谬之处，望读者批评指正。

任承俊

1985年3月13日

目　录

第一章　整数之分解

一、提　　要

定义　a为一实数，命〔a〕表示不超过a的最大整数。又命 $\{a\}=a-[a]$．〔a〕和$\{a\}$分别称为a的整数部分和小数部分。

定理1　任给二整数a及b（$b>0$），必有二整数q及r，使

$$a=qb+r,\quad 0\leqslant r<b.$$

定理2　若$b\neq 0$，$c\neq 0$，则

1）若$b|a$，$c|b$，则$c|a$；

2）若$b|a$，则$bc|ac$；

3）若$c|d$，$c|e$，则对任意的m、n有$c|dm+en$。

定理3　若b是a的真因数，则

$$1<|b|<|a|.$$

定理4　非1的自然数都可以分解为素数的乘积。

定义　称一整数集合M为模，是指M满足条件：若 $m\in M$，$n\in M$，则$m\pm n\in M$。

定理5　任何模必包含0；若a、b在模中，则$am+bn$也在模中．m、n为任何整数。

定理6　任一非零模，必为一正整数的倍数所成的集合。

定义　命a、b为二整数，于定理6中取形如$am+bn$所成的模，其中最小的正整数d称为a、b的最大公因数，记为(a,b)．

定理 7 (a,b) 有如下性质：

1）有整数x、y，使 $(a,b)=ax+by$；

2）对任何整数x、y，必有 $(a,b)|ax+by$；

3）若$e|a$，$e|b$，则$e|(a,b)$．

定义 若$(a,b)=1$，则称a、b互素．

定理 8 若p为素数并且$p|ab$，则$p|a$或$p|b$．

定理 9 若$c>0$及 $(a,b)=d$，则一定有 $(ac,bc)=dc$．

定理10 n的标准分解式是唯一的．即如果不计次序，则n仅能由唯一的方法表示为素数的乘积．

定理11 命a、b为二正整数，p_1，……，p 为其素因数．记为

$$a=p_1^{a_1}\cdots\cdots p_s^{a_s}, \qquad a_v\geqslant 0$$

$$b=p_1^{b_1}\cdots\cdots p_s^{b_s}, \qquad b_v\geqslant 0$$

则 $(a,b)=p_1^{c_1}\cdots\cdots p_s^{c_s}, c_v=\min(a_v,b_v)$．符号$\min(x_1,\cdots\cdots,x\ )$表$x_1$，……，$x_n$中最小的一个．

定义 命a、b为正整数．a、b都能整除的数称为它们的公倍数，其中最小的一个正整数名为最小公倍数，记为$[a,b]$．

定理12 与定理11的假定相同．a、b的最小公倍数为

$[a,b]=p_1^{e_1}\cdots\cdots p_s^{e_s}, e_v=\max(a\ \ ,b\ )$．符号$\max(x_1,\cdots\cdots,x\ )$表$x_1$,……，$x_n$中最大的一个．

定理13 a，b的任一公倍数必为其最小公倍数的倍数．

定理14 $$[a,b]\cdot(a,b)=ab$$

定理15 命

$$a_1=p_1^{e_{11}}\cdots\cdots p_s^{e_{1s}},\cdots\cdots,\ a_n=p_1^{e_{n1}}\cdots\cdots p_s^{e_{ns}},$$

且 $e_{\mu v}\geqslant 0$，则

$$(a_1,\cdots\cdots,a_n)=p_1^{e_1}\cdots\cdots p_s^{e_s}\quad, e_v=\min(e_{1v},\cdots\cdots,e_{nv}),$$

$$[a_1,\cdots\cdots,a_n]=p_1^{d_1}\cdots\cdots p_s^{d_s}\quad, d_v=\max(e_{1v},\cdots\cdots,e_{nv}).$$

其中 $(a_1,\cdots\cdots,a_n)=((a_1,\cdots\cdots,a_{n-1}),\ a_n)$,

$$[a_1, \cdots\cdots, a_n] = [[a_1, \cdots\cdots, a_{n-1}], a_n].$$

它们分别表示$a_1, \cdots\cdots, a$ 的最大公因数和最小公倍数。

定理16 （逐步淘汰原则）设有N件事物，其中$N\alpha$件有性质α，N_β件有性质β，……，$N_{\alpha\beta}$件同时有性质α及β，……，$N_{\alpha\beta\gamma}$件同时有性质α，β及γ，……。则此事物中既无性质α，又无性质β，又无性质γ，……的件数为

$$N - N\alpha - N\beta - \cdots\cdots + N\alpha\beta + \cdots\cdots - N\alpha\beta\gamma - \cdots\cdots + \cdots\cdots$$

定理17 方程

$$ax + by = n$$

有整数解x、y的充分必要条件为$(a,b)|n$。

定理18 若$(a,b)=1$，且x_0、y_0为方程

$$ax + by = n$$

的一组解，则$ax+by=n$的所有解为

$$x = x_0 + bt,\ y = y_0 - at.$$

定理19 设$(a,b)=1$，$a>0$，$b>0$。凡大于$ab-a-b$的数必可表示为$ax+by$的形式，但$ab-a-b$不能表示成此种形式，其中$x\geqslant 0$，$y\geqslant 0$。

定理20 命$\sigma(n)$为n的所有因数的和，如果

$$n = p_1^{a_s} \cdots\cdots p_s^{a_s}$$

则
$$\sigma(n) = \frac{p_1^{a_s+1} - 1}{p_1 - 1} \cdots\cdots \frac{p_s^{a_s+1} - 1}{p_s - 1},$$

定理21 若$(n,m)=1$，则

$$\sigma(mn) = \sigma(m)\sigma(n).$$

定义 若$\sigma(n)=2n$，则称n为完全数。

定理22 若$p=2^n-1$为素数，则

$$\frac{1}{2}p(p+1) = 2^{n-1}(2^n - 1)$$

是一个完全数，且无其它偶完全数存在。

定义 形如2^n-1的素数称为Merenne数。

定义 形如$2^{2^n}+1$的数称为Fermat数。

定理23 p为素数，在$n!$中p的方次数为

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots\cdots.$$

定理24 $\binom{n}{r}=\frac{n!}{r!(n-r)!}$为一整数。

定义 当变数x取整数时，如果多项式$f(x)$的值总是整数，则称$f(x)$为整值多项式。

定理25 设$\Delta f(x)=f(x+1)-f(x)$

则
$$\Delta\binom{x}{r}=\binom{x}{r-1}.$$

定理26 凡k次整值多项式必可表示成

$$a_k\binom{x}{k}+a_{k-1}\binom{x}{k-1}+\cdots\cdots+a_1\binom{x}{1}+a_0$$

上式中$a_k,\cdots\cdots$，a_0都是整数，且只要$a_k,\cdots\cdots$，a_0取整数，那么上式总是整值多项式。

定理27 对任意整数x，整值多项式$f(x)$是m的倍数的充分必要条件为

$$m|(a_k,\cdots\cdots,a_0).$$

此处$a_k,\cdots\cdots,a_0$定义同定理26。

定义 命$f(x)$为一有理系数多项式，若有二个非常数的有理系数多项式$q(x)$及$h(x)$使

$$f(x)=q(x)h(x)$$

则称$f(x)$可分解或可化，不然则称$f(x)$不可分解或不可化。

定理28 (Fisenstein) 命

$$f(x)=c_nx^n+\cdots+c_0$$

为一整系数多项式。若$p\nmid c_n$，$p|c_i$，$0\leqslant i<n$且$p^2\nmid c_0$，则$f(x)$不

可化。

二、题 解

§1 整除性

习题1　若n为正整数，则$\left[\frac{[n\alpha]}{n}\right]=[\alpha]$.

证：设　$[n\alpha]=nq+r$，$0\leqslant r<n$，那么

$$n\alpha=nq+r+\{n\alpha\}$$

$$\left[\frac{[n\alpha]}{n}\right]=\left[\frac{nq+r}{n}\right]=\left[q+\frac{r}{n}\right]=q$$

$$[\alpha]=\left[\frac{n\alpha}{n}\right]=\left[\frac{nq+r+\{n\alpha\}}{n}\right]$$

$$=\left[q+\frac{r+\{n\alpha\}}{n}\right]=q$$

从而　$$\left[\frac{[n\alpha]}{n}\right]=[\alpha].$$

习题2　若n为正整数，则

$$[\alpha]+\left[\alpha+\frac{1}{n}\right]+\cdots\cdots+\left[\alpha+\frac{n-1}{n}\right]=[n\alpha].$$

证：设$[n\alpha]=nq+r$，$0\leqslant r<n$，那么

$$n\alpha=nq+r+\{n\alpha\}$$

$$\alpha=q+\frac{r+\{n\alpha\}}{n}$$

当$r=0$时结论显然成立。当$r\geqslant 1$时

$$[\alpha]+\left[\alpha+\frac{1}{n}\right]+\cdots\cdots+\left[\alpha+\frac{n-1}{n}\right]$$

$$=\left[q+\frac{r+\{n\alpha\}}{n}\right]+\left[q+\frac{r+\{n\alpha\}+1}{n}\right]+\cdots\cdots$$

$$+\left[q+\frac{r+\{n\alpha\}+n-1}{n}\right]$$

$$=nq+\sum_{k=0}^{n-r-1}\left(\frac{r+\{n\alpha\}+k}{n}\right)+\sum_{k=n-r}^{n-1}\left[\frac{r+\{n\alpha\}+k}{n}\right]$$

$$=nq+0+((n-1)-(n-r)+1)$$

$$=nq+r=[n\alpha].$$

习题3 证明不等式

$$[2\alpha]+[2\beta]\geqslant[\alpha]+[\alpha+\beta]+[\beta].$$

证：设$\alpha=m+a$，$\beta=n+b$，m、n为正整数，$0\leqslant a<1$，$0\leqslant b<1$。毫无损失，可设$a\geqslant b$，那么

$$[2\alpha]+[2\beta]=[2m+2a]+[2n+2b]$$

$$=2m+2n+[2a]+[2b]$$

$$\geqslant(m+n)+(m+n)+[a+b]$$

$$=[m+a]+[n+b]+[m+n+a+b]$$

$$=[\alpha]+[\beta]+[\alpha+\beta].$$

§5 唯一分解定理

习题1 证明以下各数非有理数（有理数者乃形如$\frac{a}{b}$之数）。

$$\log_{10}2,\ \sqrt{2}.$$

证：如果$\log_{10}2=\frac{a}{b}$， $(a,b)=1$，那么

$$2=10^{\frac{a}{b}},$$

$$2^b=2^n\cdot 5^n.$$

由唯一分解定理可得$a=b=0$，与题设矛盾。

如果$\sqrt{2}=\frac{a}{b}$，$(a, b)=1$，那么

$$2=\frac{a^2}{b^2}$$

$$2b^2=a^2.$$

因此$2\mid a^2$，$2\mid a$。设$a=2a_1$就有

$$b^2=2a_1^2,\ 2\mid b^2,\ 2\mid b.$$

从而$(a, b)\geqslant 2$，与$(a, b)=1$矛盾。

习题2 若已知

$$\log_{10}\frac{1025}{1024}=a,\quad \log_{10}\frac{1024^2}{1023\cdot 1025}=b,$$

$$\log_{10}\frac{81^2}{80\cdot 82}=c,\quad \log_{10}\frac{125^2}{1124\cdot 126}=d,$$

$$\log_{10}\frac{99^2}{98\cdot 100}=e,$$

则 $$196\log_{10}2=59+5a+8b-3c-8d+4e.$$

并试用a、b、c、d、e表出$\log_{10}3$及$\log_{10}41$；再用此法求$\log_{10}2$至小数第十位，以说明此法在实际计算上有用处（已知$\log_e 10=2.3025850930$）。

证： $$a=\log_{10}\frac{1025}{1024}=\log_{10}\frac{5^2\cdot 41}{2^{10}}$$

$$5a=10\log_{10}5+5\log_{10}41-50\log_{10}2;$$

$$b=\log_{10}\frac{1024^2}{1023\cdot 1025}=\log_{10}\frac{2^{20}}{3\cdot 5^2\cdot 11\cdot 31\cdot 41}$$

$$8b = 160\log_{10}2 - 8\log_{10}3 - 16\log_{10}5 - 8\log_{10}11 - 8\log_{10}31 - 8\log_{10}41;$$

$$c = \log_{10}\frac{81^2}{80 \cdot 82} = \log_{10}\frac{3^8}{2^5 \cdot 5 \cdot 41}$$

$$-3c = 15\log_{10}2 + 3\log_{10}5 + 3\log_{10}41 - 24\log_{10}3;$$

$$d = \log_{10}\frac{125^2}{124 \cdot 126} = \log_{10}\frac{5^6}{2^3 \cdot 3^2 \cdot 7 \cdot 31}$$

$$-8d = 24\log_{10}2 + 16\log_{10}3 + 8\log_{10}7 + 8\log_{10}31 - 48\log_{10}5;$$

$$e = \log_{10}\frac{99^2}{98 \cdot 100} = \log_{10}\frac{3^4 \cdot 11^2}{2^3 \cdot 5^2 \cdot 72}$$

$$4e = 16\log_{10}3 + 8\log_{10}{}^{11} - 12\log_{10}2 - 8\log_{10}5 - 8\log_{10}7.$$

因此 $59 + 5a + 8b - 3c - 8d + 4e$

$$= 59 + 137\log_{10}2 - 59\log_{10}5$$

$$= 59 + 137\log_{10}2 - 59 + 59\log_{10}2$$

$$= 196\log_{10}2. \qquad (1)$$

由（1）有

$$588\log_{10}2 = 3 \times 196\log_{10}2$$

$$= 177 + 15a + 24b - 9c - 24d + 12e \qquad (2)$$

又因为 $a = 2 - 12\log_{10}2 + \log_{10}41$

即 $12\log_{10}2 = 2 + \log_{10}41 - a$，从而又有

$$588\log_{10}2 = 49 \times 12\log_{10}2 = 98 + 49\log_{10}41 - 49a \qquad (3)$$

由(2)、(3)有 $43\log_{10}41 = 588\log_{10}2 + 49a - 98 = 177 + 15a + 24b - 9c - 24d + 12e + 49a - 98$

$$= 177 + 15a + 24b - 9c - 24d + 12e + 49a - 98$$

$$= 79 + 64a + 24b - 9c - 24d + 12e \qquad (4)$$

由 $c = \log_{10}\frac{81^2}{80 \cdot 82} = 8\log_{10}3 - 5\log_{10}2 - \log_{10}5 - \log_{10}41$

有 $8\log_{10}3 = c + 4\log_{10}2 + \log_{10}41 + 1$

$$392\log_{10}3 = 49\times 8\log_{10}3$$
$$= 49c + 196\log_{10}2 + 49\log_{10}41 + 49 \qquad (5)$$

把（1）、（4）代入（5）得

$$392\log_{10}3 = 49c + 59 + 5a + 8b - 3c - 8d + 4e$$
$$+ 79 + 64a + 24b - 9c - 24d + 12e + 49$$
$$= 187 + 69a + 32b + 37c - 32d + 16e \qquad (6)$$

（1）、（4）、（6）即为所需的等式。下面用（1）式计算 $\log_{10}2$ 至小数第十位。由（1）有

$$\log_{10}2 = \frac{59 + 5a + 8b - 3c - 8d + 4e}{196}$$

$$\approx \frac{59 + 2121475\times 10^{-9} - 2872\times 10^{-9} - 198597\times 10^{-9}}{196}$$

$$+ \frac{-222368\times 10^{-9} + 17726\times 10^{-8}}{196}$$

$$= \frac{59.00187489}{196}$$

$$\approx 0.3010299739.$$

§6　最大公因数及最小公倍数

习题1　证明下列二等式：

$(a_1\cdots\cdots,a_n) = ((a_1,\cdots\cdots,a_s),\ (a_{+1},\cdots\cdots,a_n)),$

$[b_1,\cdots\cdots,a_n] = [[b_1,\cdots\cdots,b_s],\ [b_{+1},\cdots\cdots,b_n]].$

证： 对s行归纳法，先证明第一个等式．当$s=1$时，由定义有

$(a_1\cdots\cdots,a_n) = (a_1,\ (a_2,\cdots\cdots,a_n))$ ．

归纳假定$s=k(k<n)$时等式成立，即

$(a_1,\cdots\cdots,a_{..}) = ((a_1,\cdots\cdots,a_k),(a_{k+1},\cdots\cdots,a_n)).$

当$s=k+1$时

$$
\begin{aligned}
&((a_1,\cdots,a_k,\ a_{k+1}),\ (a_{k+2},\cdots,a_n))\\
&=(((a_1,\cdots,a_k),\ a_{k+1}),\ (a_{k+2},\cdots,a_n))\\
&=((a_1,\cdots,a_k),\ a_{k+1},\ (a_{k+2},\cdots,a_n))\\
&=((a_1,\cdots,a_k),\ (a_{k+1},\ (a_{k+2},\cdots,a_n)))\\
&=((a_1,\cdots,a_k),\ (a_{k+1},\ a_{k+2},\cdots,a_n))\\
&=(a_1,\cdots\cdots,a_n)
\end{aligned}
$$

故等式对于$s=k+1$时也成立。同理可证第二个等式。

习题 2　证明下列二式：

$$(a_1,\cdots,a_n)=\frac{a_1a_2\cdots a_n}{[a_2\cdots a\ ,a_1a_3\cdots a_n,\cdots,a_1a_3\cdots a_{n-1}]},$$

$$[a_1,\cdots,a_n]=\frac{a_1a_2\cdots a}{(a_2\cdots a\ ,a_1a_3\cdots a_n,\cdots,a_1a_3\cdots a_{n-1})}.$$

证： 先证明一个辅助等式：

$$[a_1b,\cdots,a\ b]=[a_1,\cdots,a_n]b. \qquad (1)$$

用归纳法。$n=2$时，由提要中定理14和定理9可得

$$[a_1b,a_2b]=\frac{a_1a_2b^2}{(a_1b,a_2b)}=\frac{a_1a_2b}{(a_1,a_2)}=[a_1,a_2]b,$$

即$n=2$时成立。归纳假定$n=k$时（1）成立，则当$n=k+1$时

$$
\begin{aligned}
&[a_1b,\cdots,a_kb,\ a_{k+1}b]=[[a_1b,\cdots,a_kb],\ a_{k+1}b]\\
&=[[a_1,\cdots,a_k]b,\ a_{k+1}b]=[[a_1,\cdots,a_k],\ a_{k+1}]b\\
&=[a_1,\cdots,a_k,a_{k+1}]b.
\end{aligned}
$$

因此（1）式在$n=k+1$时也成立。再证本题中第一个等式。仍用归纳法。$n=2$时，我们得到

$$(a_1,a_2)=\frac{a_1a_2}{[a_1,\ a_2]}$$

上式显然成立。设$n=k$时成立，即

$$[a_2\cdots a_k,\ a_1a_3\cdots a_k,\cdots,a_1\cdots a_{k-1}]=\frac{a_1\cdots a_k}{(a_1,\cdots,a_k)} \qquad (2)$$

当$n=k+1$时，由（1）、（2）及提要中定理9立刻得到

$$\frac{a_1\cdots a_{k+1}}{[a_2\cdots a_{k+1},a_1a_3\cdots a_{k+1},\cdots,a_1\cdots a_k]}$$

$$=\frac{a_1\cdots a_{k+1}}{[[a_2\cdots a_{k+1},\cdots,a_1\cdots a_{k-1}a_{k+1}],\ a_1\cdots a_k]}$$

$$=\frac{a_1\cdots a_{k+1}}{[[a_2\cdots a_k,\cdots,a_1\cdots a_{k-1}]a_{k+1},a_1\cdots a_k]}$$

$$=\frac{a_1\cdots a_{k+1}}{\left[\frac{a_1\cdots a_k}{(a_1,\cdots,a_k)}\cdot a_{k+1},a_1\cdots a_k\right]}$$

$$=\frac{a_1\cdots a_{k+1}}{\left[\frac{a_1\cdots a_k}{(a_1,\cdots,a_k)}\cdot a_{k+1},a_1\cdots a_k\right]}\cdot\frac{a_1\cdots a_k}{(a_1,\cdots,a_k)}\cdot\frac{(a_1,\cdots,a_k)}{a_1\cdots a_k}$$

$$=\left(\frac{a_1\cdots a_k}{(a_1,\cdots,a_k)}\cdot a_{k+1},\ a_1\cdots a_k\right)\cdot\frac{(a_1,\cdots,a_k)}{a_1\cdots a_k}$$

$$=(a_{k+1},\ (a_1,\cdots,a_k))=(a_{k+1},a_1,\cdots,a_k)=(a_1,\cdots,a_{k+1})$$

故结论对于$n=k+1$时也成立。类似地可以证明本题中第二个等式。

习题3　命$a_1,\cdots,a_n$为n个整数，则$(a_1,\cdots,a_n)$为形如$a_1x_1+\cdots+a_nx_n$诸整数所成之模中之最小正整数。

证： 设$(a_1,\cdots,a_n)=d$，，对于所给模中的任意正整数$d_1=a_1x_1+\cdots a_nx_n$，因为$d|a_1,\cdots,d|a_n$，所以$d|d_1$，$d\leqslant d_1$。下面我们只需要证明d形如$a_1x_1+\cdots+a_nx_n$就可以了。用归纳法证明如下：

当$n=2$时，$(a_1,a_2)=d$，由辗转相除法可得二整数x_1、x_2，使得$d=a_1x_1+a_2x_2$。设$n=k$时结论成立，则当$n=k+1$时

$$d=(a_1,\cdots,a_k,\ a_{k+1})=((a_1,\cdots,a_k),\ a_{k+1}),$$

对于 $(a_1,\cdots,a_k)$、a_{k+1}，存在二整数x'、x_{k+1}使得

$$d=(a_1,\cdots,a_k)x'+a_{k+1}x_{k+1} \qquad (1)$$

由归纳假定，有整数$x_1',\cdots,x_k'$使

$$(a_1,\cdots,a_k)=a_1x_1'+\cdots+a_kx_k' \qquad (2)$$

把（2）代入（1）得到

$$d=a_1x_1'x'+\cdots+a\ x_k'x'+a_{k+1}x_{k+1} \qquad (3)$$

若令 $x_i=x_i'x'$，$1\leqslant i\leqslant k$

（3）式就可以写成

$$d=a_1x_1+\cdots+a_{k+1}x_{k+1}.$$

即$n=k+1$时结论也成立，所以$(a_1,\cdots,a_n)$确实是形如$a_1x_1+\cdots+a_nx_n$诸整数所成模中最小的一个正整数。

习题 4 求出一组x、y、z，使

$$6x+15y+20z=17.$$

解： 从原方程得

$$x=2-2y-3z+\frac{5-3y-2z}{6} \qquad (1)$$

令

$$\frac{5-3y-2z}{6}=t_1$$

得

$$z=2-y-3t_1+\frac{1-y}{2} \qquad (2)$$

再令

$$\frac{1-y}{2}=t_2$$

得

$$y=1-2t_2 \qquad (3)$$

把（3）代入（2）得 $z=1-3t_1+3t_2$ （4）

把（3）、（4）代入（1）得

$$x=-3+10t_1-5t_2 \qquad (5)$$

由（3）、（4）、（5）即知

$$\begin{cases} x=-3+10t_1-5t_2 \\ y=1-2t_2 \\ z=1-3t_1+3t_2 \end{cases} \quad (6)$$

是原方程的解。其中t_1、t_2为任意整数。如果在（6）式中，取$t_1=0$、$t_2=-1$，就得到$x=2$、$y=3$、$z=-2$。此组x、y、z显然满足

$$6x+15y+20z=17.$$

习题5 今有散钱，不知其数，作七十七陌穿之，欠五十凑穿，若作七十八陌穿之，不多不少。问钱若干？

解： 设钱数为x，依题意有正整数m、n存在，使

$$x=77m-50, \quad x=78n.$$

故

$$77m-50=78n. \quad (1)$$

$$m=n+\frac{n+50}{77}$$

取$n=77k-50$，就有

$$m=78k-50$$

因此（1）的全体正整数解为

$$m=78k-50, \quad n=77k-50, \quad k\geqslant 1.$$

进而

$$x=6006k-3900.$$

可知当$k=1$时，$x=2106$为合题意的最少钱数。

§7 逐步淘汰原则

习题 命$a,b,\cdots,k,l$为正整数，求$1,2,\cdots,n$中与a, b,$\cdots$,l皆互素之整数之个数。

解： 用N 表1、$\cdots n$中与a不互素的整数的个数，$\cdots$，N_l表与l不互素的整数的个数；N_{ab}表与a、b皆不互素的整数的个数，$\cdots N_{kl}$表k、l皆不互素的整数的个数，$\cdots$，$N_{ab\cdots kl}$表与a、b,$\cdots$,l皆不互素

的整数的个数，则 1 、…，n中与a、…，l皆互素的整数个数为

$$n-N_a-\cdots-N_l+N_{al}+\cdots+N_{kl}$$
$$-\cdots+\cdots+(-1)^m N_{ab\cdots kl}.$$

其中m表整数a、b，…，k，l的个数。

§8　一次不定方程之解

习题 1　若$a>0$，$b>0$，且$(a,b)=1$，则方程

$$ax+by=n$$

之非负数解答之个数为$\left[\frac{n}{ab}\right]$或$\left[\frac{n}{ab}\right]+1$。

（提示：应用$[\alpha]-[\beta]=[\alpha]-[\beta]$或$[\alpha]-\beta+1$。）

证：设（x_0,y_0）为方程$ax+by=n$的非负解，且x_0最小。显然，方程$ax+by=n$的所有非负解由下式给出

$$\begin{cases}x=x_0+bt & x_0\geqslant -bt\\ y=y_0-at & y_0\geqslant at\end{cases}$$

如果$x_0>b$，那么在$x=x_0+bt$中取$t=-1$，就有$x=x_0-b<x_0$也是解，与x_0最小相矛盾；如果$x_0=b$，取$t=-1$，得解$x=0$，故又有$x_0=b=0$，与题设$b>0$相矛盾，因此$x_0<b$。由$x\geqslant x_0$得

$$t=\frac{x-x_0}{b}\geqslant 0 \qquad (1)$$

由$y=y_0-at$，$t=\frac{y_0}{a}-\frac{y}{a}\leqslant\frac{y_0}{a}$得

$$t\leqslant\left[\frac{y_0}{a}\right] \qquad (2)$$

合并（1）、（2）得 $0\leqslant t\leqslant\left[\frac{y_0}{a}\right]$。　　（3）

又从$\frac{y_0}{a}=\frac{n}{ab}-\frac{x_0}{b}$可得

$$\left[\frac{y_0}{a}\right]=\left[\frac{n}{ab}\right]-\left[\frac{x_0}{b}\right]\text{或}\left[\frac{n}{ab}\right]-\left[\frac{x_0}{b}\right]-1,$$

而且 $0\leqslant x_0<b$，$\left[\frac{x_0}{b}\right]=0$．因此有

$$\left[\frac{y_0}{a}\right]=\left[\frac{n}{ab}\right]\text{或}\left[\frac{n}{ab}\right]-1,$$

故（3）式给出　　$0\leqslant t\leqslant\left[\frac{n}{ab}\right]$或$\left[\frac{n}{ab}\right]-1$．

当$0\leqslant t\leqslant\left[\frac{n}{ab}\right]$时，方程有$\left[\frac{n}{ab}\right]+1$个非负解；

当$0\leqslant t\leqslant\left[\frac{n}{ab}\right]-1$时，方程有$\left[\frac{n}{ab}\right]$个非负解。

习题 2　设a、b、c为三个正整数，且

$$(a,b=(b,c)=(c,a)=1$$

求最大之整数之不可由

$$bcx+cay+abz,\ x\geqslant 0,\ y\geqslant 0,\ z\geqslant 0$$

表出者。

解：首先证明：如果方程

$$bcx+cay+abz=n,\ (a,b)=(b,c)=(c,a)=1$$

有一组解(x_0,y_0,z_0)，那么它的所有解由下式

$$\begin{cases}x=x_0+a(t_1+t_2),\\ y=y_0-bt_1,\\ z=z_0-ct_2,\end{cases}\qquad(1)$$

给出。（1）显然是方程的解．另一方面，我们从

$$bcx+cay+abz=n$$

和　　$$bcx_0+cay_0+abz_0=n$$

得到 $bc(x-x_0)+ca(y-y_0)+ab(z-z_0)=0$ （2）

再结合 $(a,b)=(b,c)=(c,a)=1$

立刻有 $a|x-x_0$，$b|y-y_0$，$c|z-z_0$，

因此 $x=x_0+aT_1$，$y=y_0+bT_2$，$z=z_0+cT_3$，

把上式代入（2）得 $T_1+T_2+T_3=0$

取$T_2=-t_1$，$T_3=-t_2$，$T_1=t_1+t_2$，即得（1）。

下面再证明合题设条件的最大不可表数是

$$2abc-ab-bc-ca.$$

命 $0\leqslant y_0-bt_1\leqslant b-1$， $0\leqslant z_0-ct_2\leqslant c-1$，

如果 $n>2abc-ab-bc-ca$

那么由 $bc(x_0+a(t_1+t_2))=n-ca(y_0-bt_1)-ab(z-z_0)$

可得

$$bc(x_0+a(t_1+t_2))>2abc-ab-bc-ca-ca(a-1)-ab(c-1)$$
$$=-bc,$$

即 $x_0+a(t_1+t_2)>-1$

故 $x_0+a(t_1+t_2)\geqslant 0$

因此，凡大于$2abc-ab-bc-ca$的整数，都可由$bcx+cay+abz$表出，其中a，b，c都是正整数，并且合条件

$(a,b)=(b,c)=(c,a)=1$，$x\geqslant 0$，$y\geqslant 0$，$z\geqslant 0$。

又若 $2abc-ab-bc-ca=bcx+cay+abz$

则 $2abc=(1+x)bc+(1+y)ac+(1+z)ab$

因为 $(a,b)=(b,c)=(c,a)=1$

所以有 $a|1+x$，$b|1+y$，$c|1+z$

再由 $x\geqslant 0$，$y\geqslant 0$，$z\geqslant 0$

可得 $1+x\geqslant a$，$1+y\geqslant b$，$1+z\geqslant c$

故 $2abc=(1+x)bc+(1+y)ac+(1+z)ab$
$\geqslant abc+abc+abc=3abc$

此不可能。因此合题设条件的最大不可表数的确是$2abc-ab-bc$

$-ca$。

习题 3 求出$x+2y+3z=n$，$x\geqslant 0$，$y\geqslant 0$，$z\geqslant 0$之解数。

提示：此式之解答数为

$$\frac{1}{(1-x)(1-x^2)(1-x^3)}$$

之展开式中x 之系数。用部分分式法可以求得。

解：由形式幂级数可知该式的解数为

$$\frac{1}{(1-x))1-x^2)(1-x^3)}$$

的展开式中x 的系数。下面来确定x 的系数。

$$\frac{1}{(1-x)(1-x^2)(1-x^3)}$$

$$=\frac{1}{(1-x)^3(1+x)(1-\omega x)(1-\omega^2 x)}$$

$$=\frac{A_1}{(1-x)^3}+\frac{A_2}{(1-x)^2}+\frac{A_3}{1-x}+\frac{A_4}{1+x}+\frac{A_5}{1-\omega x}+\frac{A_6}{1-\omega^2 x} \quad (1)$$

其中$\omega=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}$，$1+\omega+\omega^2=0$，$\omega^3=1$

而A为待定的常数。把（1）式右边通分，由特定系数法得：

$$\begin{aligned}1=&A_1(1+x)(1-\omega x)(1-\omega^2 x)\\&+A_2(1-x)(1+x)(1-\omega x)(1-\omega^2 x)\\&+A_3(1-x)^2(1+x)(1-\omega x)(1-\omega^2 x)\\&+A_4(1-x)^3(1-\omega x)(1-\omega^2 x)\\&+A_5(1-x)^3(1+x)(1-\omega^2 x)\\&+A_6(1-x)^3(1+x)(1-\omega x)\end{aligned}$$

令$x=1$，则有

$$1=2A_1(1-\omega)(1-\omega^2)=2A_1(1-\omega-\omega^2+\omega^3)=6A_1$$

$$A_1=\frac{1}{6}.$$

令$x=-1$，则有

$$1=8A_4(1+\omega)(1+\omega^2)=8A_4(1+\omega+\omega^2+\omega^3)=8A_4$$

$$A_4=\frac{1}{8}$$

令$x=\omega^2$，则有

$$1=A_5(1-\omega^2)^2(1+\omega^2)(1-\omega^4)=A_5(1-\omega-\omega^2+\omega^3)^2=9A_5$$

$$A_5=\frac{1}{9}$$

令$x=\omega$，则有

$$1=A_6(1-\omega)^3(1+\omega)(1-\omega^2)=A_6(1-2\omega+\omega^2)^2\omega^4=9A_6$$

$$A_6=\frac{1}{9}$$

下面仍用部分分式定理确定A_2和A_3。

由 $\dfrac{A_5}{1-\omega x}+\dfrac{A_6}{1-\omega^2 x}=\dfrac{1}{9}\cdot\dfrac{2-(\omega+\omega^2)x}{(1-\omega x)(1-\omega^2 x)}=\dfrac{1}{9}\cdot\dfrac{2+x}{1+x+x^2}$

及前面的计算，可把（1）式写成

$$\frac{1}{(1-x)^3(1+x)(1+x+x^2)}=\frac{1}{6(1-x)^3}+\frac{A_2}{(1-x)^2}$$

$$+\frac{A_3}{1-x}+\frac{1}{8(1+x)}+\frac{2+x}{9(1+x+x^2)}$$

分别令$x=0$，$x=2$得

$$1=\frac{1}{6}+A_2+A_3+\frac{1}{8}+\frac{2}{9}$$

$$-\frac{1}{21}=-\frac{1}{6}+A_2-A_3+\frac{1}{24}+\frac{4}{63}$$

即 $\qquad A_2+A_3=\frac{35}{72},\quad A_2-A_3=\frac{1}{72},\quad A_2=\frac{1}{4},\quad A_3=\frac{17}{72}$

故 $\frac{1}{(1-x)(1-x^2)(1-x^3)}$

$$=\frac{1}{6(1-x)^3}+\frac{1}{4(1-x)^2}+\frac{17}{72(1-x)}+\frac{1}{8(1+x)}$$

$$+\frac{1}{9(1-\omega x)}+\frac{1}{9(1-\omega^2 x)}$$

再引入下面关于无穷级数熟知的结果：

$$\frac{1}{(1-x)^3}=\sum_{n=0}^{\infty}\binom{n+2}{n}x^n \qquad \frac{1}{(1-x)^2}=\sum_{n=0}^{\infty}\binom{n+1}{n}x^n$$

$$\frac{1}{1-x}=\sum_{n=0}^{\infty}x^n \qquad \frac{1}{1+x}=\sum_{n=0}^{\infty}(-1)^n x^n$$

$$\frac{1}{1-\omega x}=\sum_{n=0}^{\infty}\omega^n x^n \qquad \frac{1}{1-\omega^2 x}=\sum_{n=0}^{\infty}\omega^{2n}x^n$$

就有 $\qquad \frac{1}{(1-x)(1-x^2)(1-x^3)}$

$$=\sum_{n=0}^{\infty}\left[\frac{1}{6}\binom{n+2}{n}+\frac{1}{4}\binom{n+1}{n}+\frac{17}{72}+\frac{(-1)^n}{8}+\frac{\omega^n}{9}+\frac{\omega^{2n}}{9}\right]x^n$$

由于 $\qquad \omega=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}$

故 $\quad \omega^n+\omega^{2n}=\cos\frac{2n\pi}{3}+i\sin\frac{2n\pi}{3}+\cos\frac{4n\pi}{3}+i\sin\frac{4n\pi}{3}$

$$=2\cos\frac{2n\pi}{3}$$

从而 $\qquad \frac{1}{6}\binom{n+2}{n}+\frac{1}{4}\binom{n+1}{n}+\frac{17}{72}+\frac{(-1)^n}{8}+\frac{\omega^n}{9}+\frac{\omega^{2n}}{9}$

$$=\frac{(n+2)(n+1)}{12}+\frac{n+1}{4}+\frac{17}{72}+\frac{(-1)^n}{8}+\frac{2}{9}\cos\frac{2n\pi}{3}$$

$$=\frac{(n+3)^2}{12}-\frac{7}{72}+\frac{(-1)^n}{8}+\frac{2}{9}\cos\frac{2n\pi}{3}$$

最后证明 $\frac{(n+3)^2}{12}-\frac{7}{72}+\frac{(-1)^n}{8}+\frac{2}{9}\cos\frac{2n\pi}{3}$ 是整数。

如果$n=3m$，由题设$m\geqslant 0$，则有

$$\frac{(n+3)^2}{12}-\frac{7}{72}+\frac{(-1)^n}{8}+\frac{2}{9}\cos\frac{2n\pi}{3}$$

$$=\frac{(3m+3)^2}{12}-\frac{7}{72}+\frac{(-1)^{3m}}{8}+\frac{2}{9}\cos\frac{6m\pi}{3}$$

$$=\frac{3(m+1)^2}{4}+\frac{(-1)^m}{8}+\frac{1}{8}$$

i）当 $2\nmid m$时　　$4\mid(m+1)^2$，$\frac{(-1)^m}{8}+\frac{1}{8}=0$；

ii）当$2\mid m$时　　$3(m+1)^2\equiv 3\pmod 4$，$\frac{(-1)^m}{8}+\frac{1}{8}=\frac{1}{4}$.

因此，当$n=3m$，$m\geqslant 0$ 时

$$\frac{(n+3)^2}{12}-\frac{7}{72}+\frac{(-1)^n}{8}+\frac{2}{9}\cos\frac{2n\pi}{3}$$

是整数。同理可证$n=3m+1$，$n=3m+2$，$m\geqslant 0$ 时，上数仍然是整数。

综上所述，我们得到了方程

$x+2y+3z=n$，$x\geqslant 0$，$y\geqslant 0$，$z\geqslant 0$ 的解数确实为：

$$\frac{(n+3)^2}{12}-\frac{7}{72}+\frac{(-1)^n}{8}+\frac{2}{9}\cos\frac{2n\pi}{3}.$$

习题 4　鸡翁一，值钱五；鸡母一，值钱三；鸡雏三，值钱一。百钱买鸡百只，问鸡翁、母、雏各几何？

解：设所买的一百只鸡中，公鸡、母鸡小鸡分别为x只、y只和z只，依题意有

$$\begin{cases} x+y+z=100, & (1) \\ 5x+3y+\frac{z}{3}=100. & (2) \end{cases}$$

（2）×3－（1）得：　　$7x+4y=100$　　（3）

$$y=25-\frac{7}{4}x=25-x-\frac{3}{4}x$$

取$x=4k$得　　$y=25-7k$

故（3）的通解为　$\begin{cases} x=4k, \\ y=25-7k. \end{cases}$

又由题意$x\geqslant 0$，$k\geqslant 0$，$y=25-7k\geqslant 0$，可知$k=0$，1，2，3。与它们相对应的方程解（x，y，z）分别为

（0，25，75）、（4，18，78）、

（8，11，81）、（12，4，84）。

故此题有四解：其一，不买公鸡，买母鸡25只，买小鸡75只；其二，买公鸡4只，买母鸡18只，买小鸡78只；其三，买公鸡8只，买母鸡11只，买小鸡81只；其四，买公鸡12只，买母鸡4只，买小鸡84只。

§9　完全数

习题1　阐明$\sigma(m)=\sigma(n)=m+n$有次之三解答：

m	284	17296	9363584
n	220	18416	9437056

解：i)$m=284$，$n=220$

$$\sigma(m)=\sigma(2^2\cdot 71)=\sigma(2^2)\sigma(71)$$

$$=\left(\frac{2^3-1}{2-1}\right)\left(\frac{71^2-1}{71-1}\right)=7\cdot 72=504$$

$$\sigma(n)=\sigma(2^2\cdot 5\cdot 11)\sigma(2^2)\sigma(5)\sigma(11)$$

$$=7\left(\frac{5^2-1}{5-1}\right)\left(\frac{11^2-1}{11-1}\right)7\cdot 6\cdot 12=504$$

$$504=284+220$$

故此时　　$\sigma(m)=\sigma(n)=m+n$

ii) $m=17296$，$n=18416$

$$\sigma(m)=\sigma(2^4\cdot 23\cdot 47)=\sigma(2^4)\sigma(23)\sigma(47)$$

$$=\left(\frac{2^5-1}{2-1}\right)\left(\frac{23^2-1}{23-1}\right)\left(\frac{47^2-1}{47-1}\right)=31\cdot 24\cdot 48=35712$$

$$\sigma(n)=\sigma(2^4\cdot 1151)=\sigma(2^4)\sigma(1151)$$

$$=\left(\frac{2^5-1}{2-1}\right)\left(\frac{1151^2-1}{1151-1}\right)=31\cdot 1152=35712$$

$$35712=17296+18416.$$

故此时　　$\sigma(m)=\sigma(n)=m+n$

iii) $m=9363584$，$n=9437056$

$$\sigma(m)=\sigma(2^7\cdot 191\cdot 383)=\sigma(2^7)\sigma(191)\sigma(383)$$

$$=\left(\frac{2^8-1}{2-1}\right)\left(\frac{191^2-1}{191-1}\right)\left(\frac{383^2-1}{383-1}\right)$$

$$=255\cdot 192\cdot 384=18800640$$

$$\sigma(n)=\sigma(2^7\cdot 73727)=\sigma(2^7)\sigma(73727)$$

$$=\left(\frac{2^8-1}{2-1}\right)\left(\frac{73727^2-1}{73727-1}\right)$$

$$=255\cdot 73728=18800640$$

$$18800640=9363584+9437056$$

故此时　　$\sigma(m)=\sigma(n)=m+n$

值得介绍：$\sigma(m)=\sigma(n)=m+n$表示m和n的真因的和相等，此种m、n称为互友数。

习题 2 求证，若一正整数为其诸因数（除其本身之外）之积，则此数为一素数之立方，或为二不同素数之积，且无其他正整数具此性质。

证 1：

i) n只含一个素因子，$n=p_1^{\alpha_1}$。令N为n的诸因数（除其本身之外）的积．显然

$$N=p_1\cdot p_1^2\cdots\cdots p_1^{\alpha_1-1}=p_1^{\frac{\alpha_1(\alpha_1-1)}{2}}$$

若$n=N$，则由唯一分解定理有

$$\alpha_1=\frac{\alpha_1(\alpha_1-1)}{2}$$

从而有，$\alpha_1=3$或0，而$\alpha_1=0$给出$n=1$，因此该种情况得到$n=p_1^3$。

ii) n含两个素因子，$n=p_1^{\alpha_1}p_2^{\alpha_2}$。此时有

$$\begin{aligned}N=&p_1\cdot(p_1p_2)\cdot(p_1p_2^2)\cdots(p_1p_2^{\alpha_2-1})\cdot(p_1p_2^{\alpha_2})\cdot\\&\cdot p_1^2\cdot(p_1^2p_2)\cdot(p_1^2p_2^2)\cdots(p_1^2p_2^{\alpha_2-1})\cdot(p_1^2p_2^{\alpha_2})\cdot\\&\cdots\cdots\qquad\cdots\cdots\qquad\cdots\cdots\\&p_1^{\alpha_1-1}\cdot(p_1^{\alpha_1-1}p_2)\cdot(p_1^{\alpha_1-1}p_2^2)\cdots(p_1^{\alpha_1-1}p_2^{\alpha_2-1})\cdot\\&(p_1^{\alpha_1-1}p_2^{\alpha_2})\cdot\\&\cdot p_1^{\alpha_1}\cdot(p_1^{\alpha_1}p_2)\cdot(p_1^{\alpha_1}p_2^2)\cdots(p_1^{\alpha_1}p_2^{\alpha_2-1})\cdot(p_2\cdot p_2^2\cdots\\&p_2^{\alpha_2}).\end{aligned}$$

如果$n=N$就有

$$p_1^{\alpha_1}=p_1^{(1+2+\cdots+\alpha_1)+[\alpha_2+2\alpha_2+\cdots+(\alpha_1-1)\alpha_2+\alpha_1(\alpha_2-1)]}$$

因此有 $$\alpha_1=\frac{\alpha_1(\alpha_1+1)}{2}+\frac{\alpha_2(\alpha_1-1)\alpha_1}{2}+\alpha_1(\alpha_2-1)$$

也就是 $$3=\alpha_1+\alpha_1\alpha_2+\alpha_2.$$

又因为$\alpha_1 \geqslant 1$，$\alpha_2 \geqslant 1$，因此$\alpha_1 = \alpha_2 = 1$，从而有$n = p_1p_2$。

iii)n含有$s(s \geqslant 3)$个素因子时，$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$。

显然$p_1^{\alpha_1} \cdot (p_1^{\alpha_1} p_i^{\alpha_i})$ 是N的一个因子，$2 \leqslant i \leqslant s$。如果$n = N$，就有$\alpha_1 \geqslant 2\alpha_1$，$\alpha_1 = 0$；同样可以证明$\alpha_2 = \alpha_3 = \cdots \alpha_s = 0$，但这与$n$有$s$（$s \geqslant 3$）个素因子的假设相矛盾。下面再给出合题设条件的数是p^3或p_1p_2、$p_1 \neq p_2$的另一个证明。

证 2：设$n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$，因为当$d$跑过$n$的全体正因数时，$\frac{n}{d}$也跑过$n$的全体正因数，所以我们可得

$$n^4 = n^2 \cdot n^2 = \prod_{d|n} d \prod_{d|n} \frac{n}{d} = \prod_{d|n} d \cdot \frac{n}{d} = \prod_{d|n} n = n^{\tau(n)}$$

故$\tau(n) = 4$，即

$$(\alpha_1 + 1) \cdots (\alpha_m + 1) = 4,$$

i)若$m = 1$，则$\alpha_1 = 3$，$n = p_1^3$；

ii)若$m = 2$，则$\alpha_1 = \alpha_2 = 1$，$n = p_1p_2$；

ii)若$m \geqslant 3$，则$\tau(n) \geqslant 6$。

所以，若n等于它的真因数的积，则$n = p^3$或$n = p_1p_2$，$p_1 \neq p_2$。

反之，如果有$n = p^3$或者$n = p_1p_2$，$p_1 \neq p_2$，则

$$\prod_{d|p^3} d = 1 \cdot p \cdot p^2 \cdot p^3 = p^6 = (p^3)^2$$

$$\prod_{d|p_1p_2} d = 1 \cdot p_1 \cdot p_2 \cdot p_1p_2 = (p_1p_2)^2$$

所以，若一正整数为其诸因数（除其本身外）的乘积，则此数定为一素数的立方，或者是两个不同素数的乘积，且无其它正整数有此性质。

§11 连乘积中素因数之方次数

习题 1 求10000！中 7 之方次数。

解： $\left[\frac{10000}{7}\right]=1428$，$\left[\frac{10000}{7^2}\right]=204$，

$\left[\frac{10000}{7^3}\right]=29$，$\left[\frac{10000}{7^4}\right]=4$，

$\left[\frac{10000}{7^5}\right]=0$。

故10000！中 7 的次数等于

$$1428+204+29+4=1665.$$

题习 2　求$\binom{1000}{500}$中 5 之方次数。

解： $\left[\frac{1000}{5}\right]=200$，$\left[\frac{1000}{5^2}\right]=40$，

$\left[\frac{1000}{5^3}\right]=8$，$\left[\frac{1000}{5^4}\right]=1$，$\left[\frac{1000}{5^5}\right]=0$；

$\left[\frac{500}{5}\right]=100$，$\left[\frac{500}{5^2}\right]=20$，$\left[\frac{500}{5^3}\right]=4$，

$\left[\frac{500}{5^4}\right]=0$。

故在$\binom{1000}{500}$中 5 的方次数等于

$$\sum_{m=1}^{\infty}\left(\left[\frac{1000}{5^m}\right]-2\left[\frac{500}{5^m}\right]\right)$$

$$=(200-2\times100)+(40-2\times20)+(8-2\times4)+(1-2\times0)=1.$$

习题 3　若$r+s+\cdots+t=n$，则

$$\frac{n!}{r!s!\cdots t!}$$

为整数。更证明若n为素数，而$\max(r, s, \cdots t) < n$，则此数为n之倍数。

证： 设$\frac{n!}{r!s!\cdots t!}$中p的方次数为N，那么

$$N=\sum_{m=1}^{\infty}\left(\left[\frac{n}{p^m}\right]-\left(\left[\frac{r}{p^m}\right]+\left[\frac{s}{p^m}\right]+\cdots+\left[\frac{t}{p^m}\right]\right)\right)$$

又因为 $$\left[\frac{n}{p^m}\right]=\left[\frac{r+s+\cdots+t}{p^m}\right]$$

$$\geqslant\left[\frac{r}{p^m}\right]+\left[\frac{s}{p^m}\right]+\cdots+\left[\frac{t}{p^m}\right]$$

从而$N\geqslant 0$，$\frac{n!}{r!s!\cdots t!}$为整数。如果$n=q$，q为素数。要证$q \mid \frac{q!}{r!s!\cdots t!}$，只需证$\frac{q!}{r!s!\cdots t!}$中$q$的方次数$\geqslant 1$即可。

因为 $$\sum_{m=1}^{\infty}\left[\frac{q}{q^m}\right]=1$$

并且在条件$\max(r, s, \cdots, t) < q$下又有

$$\sum_{m=1}^{\infty}\left[\frac{r}{q^m}\right]=\sum_{m=1}^{\infty}\left[\frac{s}{q^m}\right]=\cdots=\sum_{m=1}^{\infty}\left[\frac{t}{q^m}\right]=0$$

所以，$\frac{q!}{r!s!\cdots t!}$中q的方次数为

$$\sum_{m=1}^{\infty}\left(\left[\frac{q}{q^m}\right]-\left(\left[\frac{r}{q^m}\right]+\left[\frac{s}{q^m}\right]+\cdots+\left[\frac{t}{q^m}\right]\right)\right)$$

$$=1-0=1$$

此即$\frac{q!}{r!s!\cdots t!}$是q的倍数。

§12 整值多项式

习题 1 推广定理 2 及 3 至多变数之情形。

解：本节定理 2 及 3 如下：

定理 2 凡k次之整值多项式必可表成

$$a_k\binom{x}{k}+a_{k-1}\binom{x}{k-1}+\cdots+a_1\binom{x}{1}a_0$$

式中a_k，$\cdots a_0$皆为整数。且对任何整数a_k，$\cdots a_0$，此皆整值多项式。

定理 3 对任意整数x，一整值多项式$f(x)$之值皆为m之倍数之必要且充分条件为

$$m\mid(a_k,\ \cdots,\ a_0)$$

此处a_k，$\cdots$，a_0之意义如定理 2。

下面只作二元情形的推广(多元情形的推广与它们相类似)。

定理 2′ 二元整值多项式$f(x,\ y)$必可表成

$$a_k\binom{x}{k}+a_{k\ \ 1}\binom{x}{k-1}+\cdots+a_1\binom{x}{1}+a_0$$

式中k为$f(x,\ y)$中x的次数，a_k，$\cdots$，a_0皆为y的整值多项式，且对任何y的整值多项式a_k，$\cdots$，a_0，此皆整值多项式。

证：1)此种多项式显然是整值多项式。

2)对于二元多项式$f(x、y)$，如果它关于x的次数为k，则必可写成

$$f(x,\ y)=a_k\binom{x}{k}+a_{k-1}\binom{x}{k-1}+\cdots+a_1\binom{x}{1}+a_0$$

设 $\Delta f(x,\ y)=f(x+1,\ y)-f(x,\ y)$

显然　$\Delta f(x,\ y)=a_k\binom{x}{k-1}+a_{k-1}\binom{x}{k-2}+\cdots+a_1$

进而以$\Delta^2 f(x,y)$表$\Delta(\Delta f(x,\ y))$ 及$\Delta^r f(x,y)=\Delta(\Delta^{r-1}f(x,y))$，可立即得到

$$f(0,\ y)=a_0,\ (\Delta f(x,y))_{x=0}=a_1,\ \cdots\cdots$$

$$(\Delta^r f(x,y))_{x=0}=a_r,\ \cdots\cdots$$

若$f(x,\ y)$为整值多项式，则$\Delta f(x,\ y)$，$\Delta^2 f(x,\ y)$，……，也是整值多项式，故我们证到了

$$f(0,\ y),\ (\Delta f(x,\ y))_{x=0},\ \cdots\cdots,\ (\Delta^r f(x,\ y))_{x=0},\ \cdots\cdots$$

皆为整值多项式．也就是说，a_k，…，a_0皆为y的整值多项式．

定理 3′　对任意整数x、y，一整值多项式$f(x,\ y)$之值皆为m之倍数之必要且充分条件为

$$m\mid(a_k,\cdots,a_0)\ ;$$

此处a_k，…，a_0定义同定理2′．

证：与定理2′的证明相同．

习题 2　证明$n(n+1)(2n+1)$是 6 之倍数．

证：因为

$$n(n+1)(2n+1)=12\binom{n}{3}+18\binom{n}{2}+6\binom{n}{1}$$

$$6\mid(12,\ 18,\ 6)$$

所以$n(n+1)(2n+1)$是 6 的倍数．

习题 3　当m及n过诸正整数时，

$$m+\frac{1}{2}(m+n-1)(m+n-2)$$

亦过诸正整数，既无遗漏，也无重复．

证：设

$$1+2+\cdots+l=S_l,\ S_0=0$$

则 $$m+\frac{1}{2}(m+n-1)(m+n-2)=m+S_{m+n-2}$$

首先证明对任意正整数k，存在两个正整数m和n，使下式成立：

$$k=m+S_{m+n-2} \quad (1)$$

用归纳法证明此结论。当$k=1$时，取$m=n=1$，显然1)成立。设$k=r$时成立，即存在正整数u、v，使得

$$r=u+S_{u+v-2} \quad (2)$$

成立。由(2)得

$$r+1=u+1+S_{u+v-2}=u+1+S_{(u+1)+(v-1)-2}$$

即 $$r+1=u'+S_{u'+v'-2}$$

其中$u'=u+1$，$v'=v-1$。如果$v>1$，则$v'\geqslant 1$，结论对于$k=r+1$时成立；如果$v=1$，则有

$$r+1=u+1+S_{u-1}=1+S_u$$

$$=1+S_{1+(u+1)-2}=u''+S_{u''+v''-2}$$

其中$u''=1$、$v''=u+1$显然是正整数，故此种情形结论对于$k=r+1$时亦成立。

再证唯一性，即证对任意正整数m_1、m_2、n_1、n_2，如果

$$m_1+S_{m_1+n_1-2}=m_2+S_{m_2+n_2-2} \quad (3)$$

则一定有 $m_1=m_2$，$n_1=n_2$。

若$m_1>m_2$或$m_2>m_1$，则由(3)得

$$m_1-m_2=S_{m_2+n_2-2}-S_{m_1+n_1-2}$$

$$=(m_1+n_1-1)+(m_1+n_1)+\cdots+(m_2+n_2-2)$$

$$\geqslant m_1+n_1-1\geqslant m_1,$$

或 $$m_2-m_1=S_{m_1+n_1-2}-S_{m_2+n_2-2}$$

$$=(m_2+n_2-1)+(m_2+n_2)+\cdots+(m_1+n_1-2)$$

$$\geqslant m_2+n_2-1\geqslant m_2.$$

但以上两个不等式都与m_1、m_2是正整数这一假定相矛盾，所以

$$m_1=m_2 \quad (4)$$

把(4)代入(3)得 $S_{m_1+n_1-2}=S_{m_1+n_2-2}$

即 $\frac{1}{2}(m_1+n_1-1)(m_1+n_1-2)=\frac{1}{2}(m_1+n_2-1)$

$$\cdot(m_1+n_2-2)$$

$$n_1^2+2m_1n_1-3n_1=n_2^2+2m_1n_2-3n_2$$

$$(n_1-n_2)(n_1+n_2+2m_1-3)=0$$

如果$n_1\neq n_2$，则有$n_1+n_2+2m_1=3$，这与n_1、n_2、m_1是正整数相矛盾，因此

$$n_1=n_2 \qquad (6)$$

由(4)、(5)即得唯一性。

习题4 若一k次多项式，对于连续$k+1$个整数皆取整数值，则此多项式必为整值多项式。

证： 设

$$f(x)=a_k\binom{x}{k}+a_{k-1}\binom{x}{k-1}+\cdots+a_1\binom{x}{1}+a_0$$

是一个k次多项式，且当$x=m$，…，$m+k$时，$f(x)$都是整数。再设

$$\Delta f(x)=f(x+1)-f(x),\quad \Delta^r f(x)=\Delta(\Delta^{r-1}f(x))$$

则有 $\Delta f(x)=a_k\binom{x}{k-1}+a_{k-1}\binom{x}{k-2}+a_{k-2}$

$$\binom{x}{k-3}+\cdots+a_2\binom{x}{1}+a_1 \qquad (A_1)$$

$$\Delta^2 f(x)=a_k\binom{x}{k-2}+a_{k-1}\binom{x}{k-3}+\cdots+a_3\binom{x}{1}+a_2 \qquad (A_2)$$

…… …… …… …… …… …

$$\Delta^{k-1}f(x)=a_k\binom{x}{1}+a_{k-1} \qquad (A_{k-1})$$

$$\Delta^k f(x)=a_k \qquad (A_k)$$

及$\Delta f(x)=f(x+1)-f(x) \qquad (B_1)$

$$\Delta^2 f(x)=f(x+2)-\binom{2}{1}f(x+1)+f(x) \qquad (B_2)$$

$$\cdots\cdots \quad \cdots\cdots \quad \cdots\cdots \quad \cdots\cdots \quad \cdots$$

$$\Delta^{k-1}f(x)=f(x+k-1)-\binom{k-1}{1}f(x+k-2)+\cdots+$$

$$(-1)^{k-1}f(x) \qquad (B_{k-1})$$

$$\Delta^k f(x)=f(x+k)-\binom{k}{1}f(x+k-1)+$$

$$\cdots\cdots+(-1)^k f(x) \qquad (B_k)$$

因为$f(m)$，$f(m+1)$，$\cdots f(m+k)$都是整数，从而（A_k）和(B_k)给出

$$a_k=(\Delta^k f(x))_{x=m}$$

是整数；由于a_k是整数，因此(A_{k-1})和(B_{k-1})推出

$$a_{k-1}=(\Delta^{k-1}f(x))_{x=m}-a_k\binom{m}{1}$$

是整数；……最后，因为a_k，…，a_2是整数，所以(A_1)和(B_1)给出

$$a_1=(\Delta f(x))_{x=m}-a_k\binom{m}{k-1}-\cdots-a_2\binom{m}{1}$$

仍然是整数。又因为

$$a_0=f(m)-a_k\binom{m}{k}-\cdots-a_1\binom{m}{1}$$

显然是整数，故a_i（$0\leqslant i\leqslant k$）是整数，$f(x)$是一个整值多项式。

习题5　若$f(-x)=-f(x)$，则$f(x)$名为奇多项式，整值奇多项式之形式为

$$a_1\binom{x}{1}+a_2\binom{x+1}{3}+\cdots+a_m\binom{x+m-1}{2m-1}$$

此处a_1，…，a_m为整数。

证：奇整值多项式$f(x)$有如下形式

$$f(x)=b_1x+b_2x^3+\cdots+b_mx^{2m-1}$$

如果令 $a_1=f(1)$

$$a_r=f(r)-a_1\binom{r}{1}-a_2\binom{r+1}{3}-\cdots-a_{r-1}\binom{2r-2}{2r-3}$$

$2\leqslant r\leqslant m$,

则 $f(x)=a_1\binom{x}{1}+a_2\binom{x+1}{3}+\cdots+a_m\binom{x+m-1}{2m-1}$

因为在$b_1x+\cdots+b_mx^{2m-1}=a_1\binom{x}{1}+\cdots+a_m\binom{x+m-1}{2m-1}$中，

取$x=1$，得$a_1=f(1)$；

取$x=2$，得$a_2=f(2)-a_1\binom{2}{1}$；

…… ……；

取$x=m$，得$a_m=f(m)-a_1\binom{m}{1}-\cdots-a_{m-1}\binom{2m-2}{2m-3}$.

下面再证明a_1，…，a_m都是整数。由于$f(x)$是整值多项式，因此

$$a_1=f(1)$$

是整数；由a_1，$f(2)$是整数又可推出

$$a_2=f(2)-a_1\binom{2}{1}$$

是整数，……最后由a_1，…，a_{m-1}，$f(m)$是整数推出

$$a_m=f(m)-a_1\binom{m}{1}-a_2\binom{m+1}{3}-\cdots-a_{m-1}\binom{2m-2}{2m-3}$$

也是整数。

习题 6 若$f(-x)=f(x)$，则$f(x)$名为偶多项式。整值偶多项式之形式为

$$a_0+a_1\frac{x}{1}\binom{x}{1}+a_2\frac{x}{2}\binom{x+1}{3}+\cdots+a_m\frac{x}{m}\binom{x+m-1}{2m-1}.$$

此处a_1，…，a_m为整数。

证： 偶整值多项式$f(x)$有如下形式

$$f(x)=b_0+b_1x^2+b_2x^4+\cdots+b_mx^{2m}$$

如果令 $a_0=f(0)$

$$a_1=f(1)-a_0$$

$$a_r=f(r)-a_0-a_1\frac{r}{1}\binom{r}{1}-a_2\frac{r}{2}\binom{r+1}{3}-\cdots-a_{r-1}\frac{r}{r-1}\cdot\binom{2r-2}{2r-3}$$

$$2\leqslant r\leqslant m$$

则 $$f(x)=a_0+a_1\frac{x}{1}\binom{x}{1}+a_2\frac{x}{2}\binom{x+1}{3}+\cdots+a_m\frac{x}{m}\cdot\binom{x+m-1}{2m-1}$$

因为在 $b_0+\cdots+b_mx^{2m}=a_0+\cdots+a_m\frac{x}{m}\binom{x+m-1}{2m-1}$中，

取$x=0$，得$a_0=f(0)$；
取$x=1$，得$a_1=f(1)-a_0$；

…… ……

取$x=m$，得$a_m=f(m)-a_0-a_1\frac{m}{1}\binom{m}{1}-a_2\frac{m}{2}\binom{m+1}{3}-\cdots-$

$$a_{m-1}\frac{m}{m-1}\binom{2m-2}{2m-3}.$$

由于 $\frac{x}{k}\binom{x+k-1}{2k-1}=\frac{x(x+(k-1))}{k}$

$\frac{(x+(k-2))\cdots(x+1)x(x-1)\cdots(x-(k-2))(x-(k-1))}{(2k-1)!}$

是一个关于x的$2k$次多项式，并且当$x=0$，± 1，…，$\pm(k-1)$时，$\frac{x}{k}\binom{x+k-1}{2k+1}=0$；当$x=\pm k$时，$\frac{x}{k}\binom{x+k-1}{2k-1}=1$。所以从习题4的结论知$\frac{x}{k}\binom{x+k-1}{2k-1}$是一个整值多项式。利用此点，下面证明$a_0$，$a_1$，…，$a_m$都是整数。由于$f(x)$是整值多项式，因此

$$a_0=f(0)$$

是整数；由a_0、$f(1)$是整数又可推出

$$a_1=f(1)-a_0$$

是整数；再由a_0，a_1，$\frac{2}{1}\binom{2}{1}$，$f(2)$是整数可知

$$a_2=f(2)-a_0-a_1\frac{2}{1}\binom{2}{1}$$

是整数；……最后，由a_0，…，a_m，$\frac{m}{1}\binom{m}{1}$，…，$\frac{m}{m-1}\cdot\binom{2m-2}{2m-3}$和$f(m)$都是整数可推得

$$a_m=f(m)-a_0-a_1\frac{m}{1}\binom{m}{1}-\cdots-a_{m-1}\frac{m}{m-1}\binom{2m-2}{2m-3}$$

仍然是整数。

§13 多项式之分解

习题 证明次之诸式皆不可化：

$$x^2+1, \quad x^4+1, \quad x^6+x^3+1.$$

证： 设$x=y+1$

则 $x^2+1=y^2+2y+2$

$2\nmid 1$，$2\mid 2$，$2^2\nmid 2$，故x^2+1不可化；

而 $x^4+1=y^4+4y^3+6y^2+4y+2$

$2\nmid 1$，$2\mid 4$，$2\mid 6$，$2\mid 2$，$2^2\nmid 2$

故x^4+1不可化；

又 $x^6+x^3+1=y^6+6y^5+15y^4+21y^3+18y^2+9y+3$

$3\mid 6$，$3\mid 15$，$3\mid 21$，$3\mid 18$，$3\mid 9$，$3\mid 3$，$3^2\nmid 3$

故x^6+x^3+1不可化。

第二章　同余式

一、提　　要

定义　命m为一自然数．若$a-b$是m的倍数，则称a，b对模m同余，记为

$$a\equiv b(\bmod m).$$

定理 1

i) $a\equiv a(\bmod m)$；

ii) 若$a\equiv b$，则$b\equiv a(\bmod m)$；

iii) 若$a\equiv b$，$b\equiv c$，则$a\equiv c(\bmod m)$．

定理 2　若$a\equiv b$，$a_1\equiv b_1(\bmod m)$

则有　$a\pm a_1\equiv b\pm b_1(\bmod m)$，

及　$aa_1\equiv bb_1(\bmod m)$．

定理 3　若$ac\equiv bd(\bmod m)$，　$c\equiv d(\bmod m)$

及　$$(c,\ m)=1$$

则　$$a\equiv b(\bmod m).$$

定义　对于模m同余的数组成由模m决定的数类，而对于模m两两不同余的m个数，称为模m的完全剩余组．

定义　命$\varphi(m)$为与m互素的类的个数，此$\varphi(m)$名为欧拉函数．在与m互素的诸类中各取一代表$a_1,\cdots,a_{\varphi(m)}$，此名为一缩剩余系，或者简称为缩系．

定理 4　如果$(k,\ m)=1$，则

$$k^{\varphi(m)} \equiv 1 \pmod{m} .$$

定理 5 如果 $(m, m')=1$，则

$$\varphi(mm')=\varphi(m)\varphi(m');$$

即$\varphi(m)$为一积性函数。

定理 6

$$\varphi(p^l)=p^l(1-\frac{1}{p}),$$

$$\varphi(m)=m\prod_{p|m}(1-\frac{1}{p}).$$

定理 7 （孙子定理）若$(m_i, m_j)=1$，$(i\neq j)$，

则 $x\equiv a_i \pmod{m_i}$，$1\leqslant i\leqslant n$

有唯一解$\bmod m_1\cdots m_n$。

定理 8 若 $(m_1, m_2)=1$，

则同余方程 $f(x)\equiv 0 \pmod{m_1m_2}$

的解数为二方程

$$f(x)\equiv 0 \pmod{m_1},\quad f(x)\equiv 0 \pmod{m_2}$$

的解数的积。

定理 9 命p为素数，同余方程

$$f(x)=a_n x^n+\cdots+a_0\equiv 0 \pmod{p}$$

的解数$\leqslant n$，重解计算在内。

定理10 正整数p为素数的充要条件为

$$(p-1)!\equiv -1 \pmod{p}.$$

定理11 命

$$f'(x)=na_n x^{n-1}+\cdots+2a_2x+a_1,$$

若 $f(x)\equiv 0$，$f'(x)\equiv 0 \pmod{p}$

无公共解，则 $f(x)\equiv 0 \pmod{p^l}$

的解数等于$f(x)\equiv 0 \pmod{p}$的解数。

二、题　解

§5　φ(m)之讨论

习题 1　证明

$$\sum_{d|m}\varphi(d)=m,$$

式中$\sum\limits_{d|m}$表示一和，其中之变数d过m之诸因数。

证： 设$m=p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s}$，

则 $$\sum_{d|m}\varphi(d)=\sum_{x_1=0}^{l_1}\sum_{x_2=0}^{l_2}\cdots\sum_{x_s=0}^{l_s}\varphi(p_1^{x_1}p_2^{x_2}\cdots p_s^{x_s})$$

$$=\sum_{x_1=0}^{l_1}\varphi(p_1^{x_1})\sum_{x_2=0}^{l_2}\varphi(p_2^{x_2})\cdots\sum_{x_s=0}^{l_s}\varphi(p_s^{x_s})$$

$$=[1+(p_1-1)+(p_1^2-p_1)+\cdots+(p_1^{l_1}-p_1^{l_1-1})]\cdot$$
$$[1+(p_2-1)+(p_2^2-p_2)+\cdots+(p_2^{l_2}-p_2^{l_2-1})]\cdots$$
$$[1+(p_s-1)+(p_s^2-p_s)+\cdots+(p_s^{l_s}-p_s^{l_s-1})]$$

$$=p_1^{l_1}\cdot p_2^{l_2}\cdots p_s^{l_s}$$

$$=m.$$

习题 2　命P为$(m,\ n)$中不同素因数之积，

则

$$\frac{\varphi(mn)}{\varphi(m)\varphi(n)}=\frac{P}{\varphi(P)}.$$

证：

$$\frac{\varphi(mn)}{\varphi(m)\varphi(n)}=\frac{mn\prod\limits_{p|mn}\left(1-\frac{1}{p}\right)}{m\prod\limits_{p|m}\left(1-\frac{1}{p}\right)\ n\prod\limits_{p|n}\left(1-\frac{1}{p}\right)}$$

$$=\frac{\prod\limits_{p|mn}\left(1-\frac{1}{p}\right)}{\prod\limits_{p|m}\left(1-\frac{1}{p}\right)\prod\limits_{p|n}\left(1-\frac{1}{p}\right)}$$

$$=\frac{1}{\prod\limits_{p|P}\left(1-\frac{1}{p}\right)}$$

$$=\frac{P}{p\prod\limits_{p|P}\left(1-\frac{1}{p}\right)}$$

$$=\frac{P}{\varphi(P)}.$$

习题 3　应用定理1.7.1证明定理 4 .

证：此题就是要求用逐步淘汰法则证明

$$\varphi(m)=m\prod_{p|m}\left(1-\frac{1}{p}\right).$$

设 $$m=p_1^{a_1}\cdots p_s^{a_s}$$

用Np_1表 1 , …, m中不与 p_1互素的整数的个数, …, 用 Np_s 表不与p_s互素的整数的个数; 用 Np_1p_2 表不与p_1, p_2互素的整数的个数, …,用$Np_{s-1}p_s$表不与p_{s-1}、p 互素的整数的个数; …; 用$Np_1\cdots p_s$表不与p_1, …, p 互素的整数的个数。显然,

$$N_{p_1}=\frac{m}{p_1},\quad \cdots,\quad N_{p_s}=\frac{m}{p_s}$$

$$N_{p_1\cdots p_s}=\frac{m}{p_1\cdots p_s}.$$

由逐步淘汰法则可知，1，2，…，m中与m互素的整数个数为

$$m-\frac{m}{p_1}-\cdots-\frac{m}{p_s}+\frac{m}{p_1p_2}+\cdots+\frac{m}{p_{s-1}p_s}-\frac{m}{p_1p_2p_3}$$

$$-\cdots+\cdots+(-1)^s\frac{m}{p_1\cdots p_s}$$

$$=m\prod_{p|m}(1-\frac{1}{p}),$$

此即 $\varphi(m)=m\prod_{p|m}(1-\frac{1}{p})$.

§7 孙子定理

习题 1 换3、5、7为3、7、11，以求与70、21、15所对应之数。

解：由 $y_1\cdot3\cdot7\equiv1\pmod{11}$，$y_1\equiv10\pmod{11}$，取$y_1=10$得，被3、7整除，被11除余1的数为

$$10\cdot3\cdot7=210;$$

由 $y_2\cdot3\cdot11\equiv1\pmod 7$，$y_2\equiv3\pmod 7$，

取$y_2=3$得，被3、11整除，被7除余1的数为

$$3\cdot3\cdot11=99;$$

由 $y_3\cdot7\cdot11\equiv1\pmod 3$，$y_3\equiv2\pmod 3$，

取$y_3=2$得，被7、11整除，被3除余1的数为

$$2\cdot7\cdot11=154.$$

求得与70、21、15所对应的数是210、99、154。

习题 2 七数剩一，八数剩二，九数剩三，问本数。

解：设此数为x，并设$m_1=7$，$m_2=8$，$m_3=9$。依题意得

$$x\equiv 1\ (\mathrm{mod}\, m_1)$$
$$x\equiv 2\ (\mathrm{mod}\, m_2)$$
$$x\equiv 3\ (\mathrm{mod}\, m_3)$$

令 $M=m_1m_2m_3=m_1M_1=m_2M_2=m_3M_3$

由 $M_1'M_1\equiv 1\ (\mathrm{mod}\, m_1)$，$M_1'\cdot 8\cdot 9\equiv 1\ (\mathrm{mod}\, 7)$

有 $M_1'\equiv 4\ (\mathrm{mod}\, 7)$

由 $M_2'M_2\equiv 1\ (\mathrm{mod}\, m_2)$，$M_2'\cdot 7\cdot 9\equiv 1\ (\mathrm{mod}\, 8)$

有 $M'_2\equiv 7\ (\mathrm{mod}\, 8)$

由 $M_3'M_3\equiv 1\ (\mathrm{mod}\, m_3)$，$M_3'\cdot 7\cdot 8\equiv 1\ (\mathrm{mod}\, 9)$

有 $M'_3\equiv 5\ (\mathrm{mod}\, 9)$

取 $x\equiv 1\cdot M_1'\cdot M_1+2\cdot M'_2\cdot M_2+3\cdot M_3'\cdot M_3$

$\equiv 4\cdot 8\cdot 9+2\cdot 7\cdot 7\cdot 9+3\cdot 5\cdot 7\cdot 8$

$\equiv 288+882+840$

$\equiv 498(\mathrm{mod}\, 7\cdot 8\cdot 9)$

此即合题意的最小正整数。

习题3 十一数余三，十二数余二，十三数余一，问本数。

解：设此数为x，并设$m_1=11$，$m_2=12$，$M_3=13$。依题意得

$$x\equiv 3\ (\mathrm{mod}\, m_1)$$
$$x\equiv 2\ (\mathrm{mod}\, m_2)$$
$$x\equiv 1\ (\mathrm{mod}\, m_3)$$

令 $M=m_1m_2m_3=m_1M_1=m_2M_2=m_3M_3$

由 $M_1'M_1\equiv 1\ (\mathrm{mod}\, m_1)$，$M_1'\cdot 12\cdot 13\equiv 1\ (\mathrm{mod}\, 11)$

有 $M'_1\equiv 6\ (\mathrm{mod}\, 11)$；

由 $M_2'M_2\equiv 1\ (\mathrm{mod}\, M_2)$，$M'_2\cdot 11\cdot 13\equiv 1\ (\mathrm{mod}\, 12)$

有 $M'_2\equiv 11(\mathrm{mod}\, 12)$；

由 $M_3'\equiv 1\ (\mathrm{mod}\, m_3)$，$M_3'\cdot 11\cdot 12\equiv 1\ (\mathrm{mod}\, 13)$

有 $M'_3\equiv 7\ (\mathrm{mod}\, 13)$。

取　$x \equiv 3 \cdot M_1' \cdot M_1 + 2 \cdot M'_2 \cdot M_2 + M_3' \cdot M_3$

$\equiv 3 \cdot 6 \cdot 12 \cdot 13 + 2 \cdot 11 \cdot 11 \cdot 13 + 7 \cdot 11 \cdot 12$

$\equiv 2808 + 3146 + 924$

$\equiv 14 (\bmod 11 \cdot 12 \cdot 13)$.

此即合题意的最小正整数。

习题4　二数余一，五数余二，七数余三，九数余四，问本数。

解：设此数为x，并且$m_1 = 2$，$m_2 = 5$，$m_3 = 7$，$m_4 = 9$．依题意得

$$x \equiv 1 (\bmod m_1), \quad x \equiv 2 (\bmod m_2),$$

$$x \equiv 3 (\bmod m_3), \quad x \equiv 4 (\bmod m_4).$$

令　$M = m_1 m_2 m_3 m_4 = m_1 M_1 = m_2 M_2 = M_3 M_3 = m_4 M_4$

由　$M_1' M_1 \equiv 1 (\bmod m_1)$，$M_1' \cdot 5 \cdot 7 \cdot 9 \equiv 1 (\bmod 2)$

有　$M_1' \equiv 1 (\bmod 2)$；

由　$M_2' M_2 \equiv 1 (\bmod m_2)$，$M' \cdot 2 \cdot 7 \cdot 9 \equiv 1 (\bmod 5)$

有　$M_2' \equiv 1 (\bmod 5)$；

由　$M_3' M_3 \equiv 1 (\bmod m_3)$，$M_3' \cdot 2 \cdot 5 \cdot 9 \equiv 1 (\bmod 7)$

有　$M_3' \equiv 6 (\bmod 7)$；

由　$M_4' M_4 \equiv 1 (\bmod m_4)$，$M_4' \cdot 2 \cdot 5 \cdot 7 \equiv 1 (\bmod 9)$

有　$M_4' \equiv 4 (\bmod 9)$．

取　$x \equiv M_1' \cdot M_1 + 2 \cdot M_2' \cdot M_2 + 3 \cdot M_3' M_3 + 4 \cdot M_4' \cdot M_4$

$\equiv 315 + 252 + 1620 + 1120$

$\equiv 157 (\bmod 2 \cdot 5 \cdot 7 \cdot 9)$

此即合题意的最小正整数。

习题5　今有数不知总，以五累减之无剩，以七百十五累减之剩十，以二百四十七累减之剩一百四十，以三百九十一累减之剩二百四十五，以一百八十七累减之剩一百零九．题总数若干．

解：设总数为x，依题意得同余方程组

$$\begin{cases} x\equiv 0 \pmod 5 & (1)\\ x\equiv 10 \pmod{715} & (2)\\ x\equiv 140 \pmod{247} & (3)\\ x\equiv 245 \pmod{391} & (4)\\ x\equiv 109 \pmod{187} & (5)\end{cases}$$

由(2)有　　$x=715y+10$　　(6)

将(6)代入(3)得

$$715y+10\equiv 140 \pmod{247}$$
$$11y\equiv 2 \pmod{19}$$
$$y\equiv 14 \pmod{19}$$

由(6)得　　$x\equiv 715\cdot 14+10$

$$\equiv 10020 \pmod{715\cdot 19}$$

即$x=10020$是适合(2)、(3)的最小正整数解．另一方面有

$10020\equiv 0 \pmod 5$，$10020\equiv 245 \pmod{391}$，

$10020\equiv 109 \pmod{187}$．

即$x=10020$适合(1)、(4)、(5)．故$x=10020$是合题意的最小正整数解。

第三章　二次剩余

一、提　要

定义　设m为大于1的整数，$(m, n)=1$，

若

$$x^2 \equiv n(\bmod m)$$

可解，则n称为对模m的二次剩余，或二次剩余mod$m$；不然则称为对模m的二次非剩余。

定义　（Legendre符号）设p为大于2的素数，$p \nmid n$，命

$$\left(\frac{n}{p}\right)=\begin{cases}1 & \text{若}n\text{为二次剩余，}\bmod p\\ -1 & \text{若}n\text{为二次非剩余，}\bmod p\end{cases}$$

此符号显然有如下性质：若$n \equiv n'(\bmod p)$及$p \nmid n$，则

$$\left(\frac{n}{p}\right)=\left(\frac{n'}{p}\right).$$

定理1　命$p>2$，于一缩系mod$p$中，有$\frac{1}{2}(p-1)$个二次剩余和$\frac{1}{2}(p-1)$个二次非剩余，

且

$$1^2,\ 2^2,\ \cdots,\ \left(\frac{1}{2}(p-1)\right)^2$$

即为其诸二次剩余mod$p$。

定理 2　(Euler判别条件) 设p是一奇素数，则

$$n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) \pmod{p} .$$

定理 3　若$p \nmid mn$，则

$$\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)=\left(\frac{mn}{p}\right)$$

定理 4　(Gauss)命$p>2$，$p \nmid n$。设 $\frac{1}{2}(p-1)$ 个数

$$n,\ 2n,\ \cdots,\ \frac{1}{2}(p-1)n \qquad (\bmod p)$$

的最小正剩余中有m个大于 $\frac{1}{2}p$，则

$$\left(\frac{n}{p}\right)=(-1)^m.$$

定理 5　若$p>2$，则

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}},\ \left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

定理 6　(互逆定律) 命$p>2$，$q>2$为二个素数，且$p \neq q$，则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}.$$

定理 7　命$l>0$，$p \nmid n$，若$p>2$，则同余式

$$x^2 \equiv n \pmod{p^l}$$

的解数为 $1+\left(\frac{n}{p}\right)$.

定义　命m的标准分解式为

$$m=\prod_{r=1}^{t}p_r,$$

其中p_r 准许重复。若 $(m,\ n)=1$，则定义

$$\left(\frac{n}{m}\right)=\prod_{r=1}^{t}\left(\frac{n}{p_r}\right).$$

此称为Jacobi符号。

特别注意，$\left(\frac{n}{m}\right)=1$ 并不说明同余式

$$x^2\equiv n(\bmod m)$$

可解。

定理 8　（计算法则）设m、m'为正奇数。

1)若$n\equiv n'(\bmod m)$ 及 $(n,\ m)=1$，则$\left(\frac{n}{m}\right)=\left(\frac{n'}{m}\right)$；

2)若 $(n,\ m)=(n,\ m')=1$，则 $\left(\frac{n}{m}\right)\left(\frac{n}{m'}\right)=\left(\frac{n}{mm'}\right)$；

3)若 $(n,\ m)=(n',m)=1$，则$\left(\frac{n}{m}\right)\left(\frac{n'}{m}\right)=\left(\frac{nn'}{m}\right)$.

定理 9　若m、n为二正奇数且 $(m,\ n)=1$，
则

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{1}{2}(n-1)\cdot\frac{1}{2}(m-1)}.$$

定理10　设m、n为奇数，$(n,\ m)=1$；若m、n皆为负数，则

$$\left(\frac{n}{|m|}\right)\left(\frac{m}{|n|}\right)=-(-1)^{\frac{1}{2}(m-1)\cdot\frac{1}{2}(n-1)}$$

不然其结果为

$$(-1)^{\frac{1}{2}(m-1)\cdot\frac{1}{2}(n-1)}.$$

定理11 $\left(\frac{-1}{m}\right)=(-1)^{\frac{1}{2}(m-1)}$,

$$\left(\frac{2}{m}\right)=(-1)^{\frac{1}{8}(m^2-1)}.$$

定理12 同余式

$$x^k\equiv n(\text{mod}p)$$

的根数为 $(k, p-1)$.

定理13 二项同余式

$$x^k\equiv n(\text{mod}p),\quad p\nmid n,$$

或无解，或有 $(k, p-1)$ 个不同的解。

定义 设h为一整数，$(n, h)=1$，最小的正整数l使

$$h^l\equiv 1(\text{mod}n)$$

者，名为h对模n的次数，或h的次数，mod$n$。

定理14 若$h^m\equiv 1(\text{mod}n)$，则$l|m$。

定义 次数为$p-1$的数，称为p的原根。如果q为p的一个原根，则

$$q^0,\ q^1,\ \cdots,\ q^{p-2}$$

中必无两个互相同余，mod$p$。

定义 任一整数n，$p\nmid n$，必有一数a，使得

$$n\equiv q^a(\text{mod}p),\quad 0\leqslant a<p-1$$

成立。此a称为n的指数，mod$p$。用$a=\text{ind}_q n$表示，也可简记为$a=\text{ind}n$。

如果b为任一数使得$n\equiv q^b(\text{mod}p)$，则

$$b\equiv\text{ind}n(\text{mod}p-1).$$

指数与通常的对数相仿，有如下性质：

1)$\text{ind}ab\equiv\text{ind}a+\text{ind}b$, $(\text{mod}\,p-1)$, $p\nmid ab$;

2)$\text{ind}a^l\equiv l\,\text{ind}a$, $(\text{mod}\,p-1)$, $p\nmid a$.

特别注意，仅当$p\nmid a$时$\text{ind}a$才有意义，此与不定义log0相同.

定义　命$p\nmid n$. 若

$$x^k\equiv n(\text{mod}\,p)$$

有解，则称n为p的k次剩余，不然则称n为p的k次非剩余.

定理15　n为p的k次剩余的必要且充分条件为

$$(k,\ p-1)|\text{ind}n.$$

定理16　m有原根存在的必要且充分条件为

$$m=2,\ 4,\ p^l,\ 2p^l;$$

此处p为奇素数.

二、题　　解

§2　计算法则

习题　若$n>0$，$4n+3$，$8n+7$皆为素数，$2^{4n+3}-1=M_{4n+3}$非素数. 由此证明以下的关于Mersenne数之性质:

$23|M_{11}$,　$47|M_{23}$,　$167|M_{83}$,　$263|M_{131}$,

$359|M_{179}$,　$383|M_{191}$,　$479|M_{239}$,　$503|M_{251}$.

证: 不难计算，当p为23、47、167、263、359、383、479、503时:

$$\left(\frac{-1}{p}\right)=-1,\ \left(\frac{2}{p}\right)=1,\ \left(\frac{-2}{p}\right)=-1.$$

下面只证明$23|M_{11}$，$503|M_{251}$，其余同理可证.

由Euler定理

$$2^{\varphi(23)}\equiv1\ (\text{mod}\,23)$$

$$2^{22} \equiv 1 \pmod{23}$$

$$(2^{11}+1)(2^{11}-1) \equiv 0 \pmod{23}$$

显然 $(2^{11}+1,\ 2^{11}-1)=1$

如果$2^{11}+1 \equiv 0 \pmod{23}$，那么

$$2^{11} \equiv -1 \pmod{23}$$

$$(2^{6})^{2} \equiv -2 \pmod{23}$$

但$\left(\frac{-2}{23}\right)=-1$，矛盾。故有

$$2^{11}-1 \equiv 0 \pmod{23}$$

即 $23 \mid M_{11}$

由Euler定理 $2^{\varphi(503)} \equiv 1 \pmod{503}$

$$2^{502} \equiv 1 \pmod{503}$$

$$(2^{251}+1)(2^{251}-1) \equiv 0 \pmod{503}$$

显然 $(2^{251}+1,\ 2^{251}-1)=1$

如果 $2^{251}+1 \equiv 0 \pmod{503}$，那么

$$2^{251} \equiv -1 \pmod{503}$$

$$(2^{126}) \equiv -2 \pmod{503}$$

但$\left(\frac{-2}{503}\right)=-1$，矛盾。故有

$$2^{251}-1 \equiv 0 \pmod{503}$$

即 $503 \mid M_{251}$

§3 互逆定律

习题1 证 $\left(\frac{3}{73}\right)=1$，$\left(\frac{17}{73}\right)=-1$。

证： $\left(\frac{3}{73}\right)=\left(\frac{73}{3}\right)(-1)^{\frac{1}{2}(73-1)\frac{1}{2}(3-1)}=\left(\frac{1}{3}\right)$

$$\cdot(-1)^{36} = \left(\frac{1}{3}\right) = 1$$

$$\left(\frac{17}{73}\right) = \left(\frac{73}{17}\right)(-1)^{\frac{1}{2}(73-1)\frac{1}{2}(17-1)} = \left(\frac{5}{17}\right)$$

$$= \left(\frac{17}{5}\right)(-1)^{\frac{1}{2}(17-1)\frac{1}{2}(5-1)} =$$

$$\left(\frac{2}{5}\right) = (-1)^{\frac{1}{8}(5^2-1)} = -1.$$

习题 2　证 $\left(\frac{195}{1901}\right) = -1$，$\left(\frac{74}{104}\right) = -1$，$\left(\frac{365}{1847}\right) = 1$。

证： $\left(\frac{195}{1901}\right) = \left(\frac{3\cdot5\cdot13}{1901}\right) = \left(\frac{3}{1901}\right)\cdot\left(\frac{5}{1901}\right)\cdot\left(\frac{13}{1901}\right)$

因为　$\left(\frac{3}{1901}\right) = \left(\frac{1901}{3}\right)(-1)^{\frac{1}{2}(1901-1)\frac{1}{2}(3-1)}$

$$= \left(\frac{2}{3}\right) = -1$$

$$\left(\frac{5}{1901}\right) = \left(\frac{1901}{5}\right)(-1)^{\frac{1}{2}(1901-1)\frac{1}{2}(5-1)}$$

$$= \left(\frac{1}{5}\right) = 1$$

$$\left(\frac{13}{1901}\right) = \left(\frac{1901}{13}\right)(-1)^{\frac{1}{2}(1901-1)\frac{1}{2}(13-1)} = \left(\frac{3}{13}\right)$$

$$=\left(\frac{13}{3}\right)(-1)^{\frac{1}{2}(13-1)\frac{1}{2}(3-1)}=\left(\frac{1}{3}\right)=1$$

故 $\left(\frac{195}{1901}\right)=(-1)\cdot 1\cdot 1=-1$；

$$\left(\frac{74}{101}\right)=\left(\frac{2\cdot 37}{101}\right)=\left(\frac{2}{101}\right)\cdot\left(\frac{37}{101}\right)$$

因为 $\left(\frac{2}{101}\right)(-1)^{\frac{1}{8}(101^2-1)}=(-1)^{1275}=-1$

$$\left(\frac{37}{101}\right)=\left(\frac{101}{37}\right)(-1)^{\frac{1}{2}(101-1)\frac{1}{2}(37-1)}=\left(\frac{27}{37}\right)$$

$$=\left(\frac{3^2\cdot 3}{37}\right)=\left(\frac{3}{37}\right)=\left(\frac{37}{3}\right)(-1)^{\frac{1}{2}(37-1)\frac{1}{2}(3-1)}$$

$$=\left(\frac{1}{3}\right)=1$$

故 $\left(\frac{74}{101}\right)=(-1)\cdot 1=-1$；

$$\left(\frac{365}{1847}\right)=\left(\frac{5\cdot 73}{1847}\right)=\left(\frac{5}{1847}\right)\cdot\left(\frac{73}{1847}\right)$$

因为 $\left(\frac{5}{1847}\right)=\left(\frac{1847}{5}\right)(-1)^{\frac{1}{2}(1847-1)\frac{1}{2}(5-1)}$

$$=\left(\frac{2}{5}\right)=(-1)^{\frac{1}{8}(5^2-1)}=-1$$

$$\left(\frac{73}{1847}\right)=\left(\frac{1847}{73}\right)(-1)^{\frac{1}{2}(1847-1)\frac{1}{2}(73-1)}=\left(\frac{22}{73}\right)$$

$$=\left(\frac{2}{73}\right)\left(\frac{11}{73}\right)=(-1)^{\frac{1}{8}(73^2-1)}\left(\frac{73}{11}\right)\cdot$$

$$(-1)^{\frac{1}{2}(73-1)\frac{1}{2}(11-1)}=(-1)^{666}\left(\frac{7}{11}\right)$$

$$=\left(\frac{11}{7}\right)(-1)^{\frac{1}{2}(11-1)\frac{1}{2}(7-1)}=\left(\frac{4}{7}\right)(-1)=-1,$$

故 $\left(\frac{365}{1847}\right)=(-1)\cdot(-1)=1$

习题 3 若 $p\equiv\pm1$ 或 $\pm5\pmod{24}$，则 $\left(\frac{6}{p}\right)=1$；

若 $p\equiv\pm7$ 或 $\pm11\pmod{24}$，则 $\left(\frac{6}{p}\right)=-1$。

证： (一) 若 $p\equiv\pm1$ 或 $\pm5\pmod{24}$，则 $\left(\frac{6}{p}\right)=1$；

1.当 $p\equiv\pm1\pmod{24}$ 时，$\left(\frac{2}{p}\right)=1$。

i) $p\equiv1\pmod{24}$ 时

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(3-1)}=\left(\frac{1}{3}\right)=1,$$

$$\left(\frac{6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)=1;$$

ii) $p\equiv-1\pmod{24}$ 时

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(3-1)}=\left(\frac{-1}{3}\right)$$

$$\cdot(-1)=1$$

$$\left(\frac{6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)=1;$$

2.当 $p\equiv\pm5\pmod{24}$ 时，$\left(\frac{2}{p}\right)=-1$。

i) $p\equiv 5 \pmod{24}$ 时

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(3-1)}=\left(\frac{2}{3}\right)=-1$$

$$\left(\frac{6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)=1$$

ii) $p\equiv -5 \pmod{24}$ 时

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(3-1)}=\left(\frac{1}{3}\right)(-1)$$

$$=-1,$$

$$\left(\frac{6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)=1.$$

（二）若 $p\equiv \pm 7$ 或 $\pm 11 \pmod{24}$，则 $\left(\frac{6}{p}\right)=-1$。

1. 当 $p\equiv \pm 7 \pmod{24}$ 时，$\left(\frac{2}{p}\right)=1$

i) $p\equiv 7 \pmod{24}$ 时

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(3-1)}=\left(\frac{1}{3}\right)(-1)$$

$$=-1$$

$$\left(\frac{6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)=-1$$

ii) $p\equiv -7 \pmod{24}$ 时

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(3-1)}=\left(\frac{2}{3}\right)=-1,$$

$$\left(\frac{6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)=-1;$$

2. 当$p\equiv\pm 11 \pmod{24}$ 时， $\left(\frac{2}{p}\right)=-1$

i) $p\equiv 11 \pmod{24}$ 时

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(3-1)}=\left(\frac{2}{3}\right)(-1)$$
$$=1$$

$$\left(\frac{6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)=-1$$

ii) $p\equiv -11 \pmod{24}$ 时

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(3-1)}=\left(\frac{1}{3}\right)=1$$

$$\left(\frac{6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)=-1.$$

§9　缩系之构造

习题　若$k<p$，$n=kp^2+1$，p为素数，且

$$2^k\not\equiv 1,\ 2^{n-1}\equiv 1 \pmod{n}$$

则n是一素数。

证：显然$1\leqslant k\leqslant p-1$。

i) n有一素因子$\equiv 1 \pmod{p}$。设2对模n的次数为d，从而有

$$2^d\equiv 1 \pmod{n}.$$

因为　$2^k\not\equiv 1 \pmod{n}$，$2^{n-1}\equiv 1 \pmod{n}$

所以　$d\nmid k$，$d|n-1$

又因为$n=kp^2+1$，所以$d|kp^2$。设k的标准分解式为

$$k=p_1^{a_1}\cdots p_s^{a_s}$$

则有　$d=p_1^{x_1}\cdots p_s^{x_s}p^l$，$0\leqslant x_i\leqslant a_i$，$1\leqslant i\leqslant s$且$l=1$或2。

因若$l=0$，$d=p_1^{x_1}\cdots p_s^{x_s}$，就有$d|k$，矛盾，从而$p|d$。又因为

$$2^{\varphi(n)} \equiv 1 \pmod{n}$$

故有$d|\varphi(n)$，$p|\varphi(n)$。设n的标准分解式为

$$n = q_1^{\alpha_1} \cdots q_t^{\alpha_t}$$

则 $$\varphi(n) = q_1^{\alpha_1 - 1} \cdots q_t^{\alpha_t - 1}(q_1 - 1)\cdots(q_t - 1)$$

因$p \nmid n$，故$p \nmid q_i^{\alpha_i - 1}$，$1 \leqslant i \leqslant t$。所以

$$p | q_j - 1, \quad 1 \leqslant j \leqslant t$$

即n有一素因子$q_j \equiv 1 \pmod{p}$。

ii)若$n = kp^2 + 1$是复合数，q为n的一个素因子且$q \equiv 1 \pmod{p}$。不妨设$q = up + 1$，$u \geqslant 1$。此时有整数$m \geqslant 2$且$n = qm$，从而$kp^2 + 1 = (up + 1)m$，$1 \equiv m \pmod{p}$，因而得知$m = vp + 1$，$v \geqslant 1$。所以

$$n = (up + 1)(vp + 1)$$

即 $$kp^2 = uvp^2 + (u + v)p \qquad (1)$$

当$k = 1$时，(1)显然不能成立。

由(1)有$u + v \equiv 0 \pmod{p}$，故$u + v \geqslant p$。如果$p = 2$，由于$k < p$，(1)显然不能成立，故有$p \geqslant 3$。此时u，v中必有一个$\geqslant 2$，不妨设$v \geqslant 2$。如果$u = 1$，则有

$$kp^2 \geqslant (p - 1)p^2 = p^3 - p^2 < p^3$$

和 $$uvp^2 + (u + v)p \geqslant (p - 1)p^2 + p \cdot p = p^3$$

故(1)式不能成立。

如果$u \geqslant 2$，从而$uv \geqslant u + v$，则有

$$kp^2 \leqslant (p - 1)p^2 < p^3$$

和 $$uvp^2 + (u + v)p \geqslant p \cdot p^2 + p \cdot p = p^3 + p^2 > p^3$$

故(1)式不能成立，即$1 < k \leqslant p - 1$时，(1)式仍然不能成立。

由i)、ii)可知，$n = kp^2 + 1$一定是素数。

（说明：原题中无“p为素数”这个条件，此条件系柯召教授在审稿中给出）

第四章　多项式之性质

一、提　　要

定义　命$f(x)$及$q(x)$为二多项式，$q(x)\neq 0$，若有一多项式$h(x)$使

$$f(x)=q(x)h(x),$$

则称$q(x)$整除$f(x)$，记为$q(x)|f(x)$或$q|f$.

定义　若$f|q$且$q|f$，则f与q仅相差一常数因子。f、q称为相结合的多项式。

定理1

1)$f|f$;

2)若$f|q$，$q|h$，则$f|h$.

3)若$f|q$，则$\partial^\circ f\leqslant\partial^\circ q$（$\partial^\circ f$，$\partial^\circ q$分别表示$f$，$q$的次数）.

定理2　任给二多项式$f(x)$与$g(x)$，$g(x)$不恒为零，必有二多项式$q(x)$及$r(x)$，使得

$$f=q\cdot g+r,\ \text{此处}r=0\ \text{或}\partial^\circ r<\partial^\circ g.$$

定义　一多项式的集合I，如适合以下条件，名为一理想集合：

1)若$f\in$I、$g\in$I，则$f+g\in$I;

2)若$f\in$I，h为任一多项式，则$fh\in$I.

定理3　任一理想集合中必可找出一多项式f，使凡此集合中的多项式必为f的倍式，即该集合由f的诸倍式组成。

定义　命f及g为二多项式，如果取形如$mf+ng$的多项式所成的集合（此处m、n皆为多项式），那么由以上定理可知此为一多项式d的倍式所成的集合。此式称为f、g的最大公因式，用$(f, g)=d$表示。为保证唯一性，规定(f, g)的最高次方系数为1。

定理 4　(f, g)有如下性质：

1)有二多项式m及n，使得$(f, g)=mf+ng$；

2)对任二多项式m及n，必有$(f, g)|nf+ng$；

3)若$l|f$，$l|g$，则$l|(f, g)$。

定义　若$(f, g)=1$，则称f，g互素。

定理 5　任一多项式皆可分解为不可化多项式的积。若相结合的多项式算作相同，并不计因子的次序，则此种分解法是唯一的。

定理 6　设$f(x)$及$g(x)$为两个具有有理系数的多项式，且$f(x)$不可化。若$f(x)=0$与$g(x)=0$有公共根，则必$f(x)|g(x)$。

定理 7　命f及g皆为最高方次系数是1的多项式：

$$f=p_1^{a_1}\cdots p_s^{a_s}\qquad a_\nu\geqslant 0$$

$$g=p_1^{b_1}\cdots p_s^{b_s}\qquad b_\nu\geqslant 0$$

式中p_ν是不相等的不可化多项式，且其最高方次系数为1，则。

$(f, g)=p_1^{c_1}\cdots p_s^{c_s}$，其中$c_\nu=\min(a_\nu, b_\nu)$。

定义　命f、g为二多项式，f及g皆能整除的多项式名为f、g的公倍式。其中次数最低的称为最小公倍式，用$[f, g]$表示最高方系数为1的最小公倍式。

定理 8　按定理7的假定，可得：

$[f, g]=p_1^{d_1}\cdots p_s^{d_s}$，其中$d_\nu=\max(a_\nu, b_\nu)$。

定理 9　二多项式的任一公倍式必为此二多项式的最小公倍式的倍式。

定理10　若f、g为首一多项式，则

$$fg=[f,\ g]\cdot(f,\ g)\ .$$

定义 命$m(x)$为一多项式，若$m(x)\mid f(x)-g(x)$，则称$f(x)$与$g(x)$对模$m(x)$同余，用$f(x)\equiv g(x)(\bmod m(x))$ 表示。

定理11

1) $f(x)\equiv f(x)(\bmod m(x))$；

2) 若$f(x)\equiv g(x)(\bmod m(x))$，则$g(x)\equiv f(x)(\bmod m(x))$；

3) 若$f(x)\equiv g(x)$，$g(x)\equiv h(x)$，则$f(x)\equiv h(x)(\bmod m(x))$；

4) 若$f(x)\equiv g(x)$，$f_1(x)\equiv g_1(x)(\bmod m(x))$，则

$$f(x)\pm f_1(x)\equiv g(x)\pm g_1(x)(\bmod m(x));$$

$$f(x)f_1(x)\equiv g(x)g_1(x)(\bmod m(x)).$$

定义 对模$m(x)$可分多项式为剩余类，每一类中的多项式皆对模$m(x)$同余，属于不同类的多项式必不同余。用O表$m(x)$所能整除的多项式所成的剩余类。

定理12 若$m(x)$不可化，则非O剩余类必有其唯一的逆类切实而言，命A表一非O剩余类，必有一类B存在，使A、B中各取一多项式$f(x)$及$g(x)$常有如下关系：

$$f(x)g(x)\equiv 1\ (\bmod m(x)).$$

定义 一组整系数（或整值）多项式，适合以下条件时，称为一理想集合：

1) 若f、g在此集合中，则$f+g$亦然；

2) 若f在此集合中，而g为任一整系数（或整值）多项式，则fg也在此集合中。

定理13 任一整系数多项式所成的理想集合A中必有有限个整系数多项式f_1，…，f_n具有如下性质：A中任一多项式必可表为

$$f=g_1f_1+g_2f_2+\cdots+g\ f_n$$

此处g_1，…g 也是整系数多项式。

定义 若二多项式$f(x)$及$g(x)$的对应系数都对模p同余，则

称此二式对模p同余，记为

$$f(x) \equiv g(x) \pmod{p}.$$

定义　$f(x)$的最高方系数非p的倍数者，称为此多项式对模p的次数，以$\partial^{\circ} f$表示。

定理14

1) $f(x) \equiv f(x) \pmod{p}$；

2) 若$f(x) \equiv g(x)$，则$g(x) \equiv f(x) \pmod{p}$；

3) 若$f(x) \equiv g(x)$，$g(x) \equiv h(x)$，则$f(x) \equiv h(x) \pmod{p}$；

4) 若$f(x) \equiv g(x)$，$f_1(x) \equiv g_1(x) \pmod{p}$，则

$$f(x) \pm f_1(x) \equiv g(x) \pm g_1(x) \pmod{p};$$

$$f(x) f_1(x) \equiv g(x) g_1(x) \pmod{p}.$$

特别注意：$(f(x))^p \equiv f(x^p) \pmod{p}$.

定义　命$f(x)$，$g(x)$为二多项式，$g(x)$不恒为零，mod$p$。若有一多项式$h(x)$使

$$f(x) \equiv h(x) g(x) \pmod{p}$$

则称$g(x)$可整除$f(x)$，mod$p$。而称$g(x)$为$f(x)$的因式，mod$p$，用$g(x) \mid f(x)$，mod$p$表示。如果存在整数a使得

$$f(x) \equiv a g(x) \pmod{p}$$

则称$f(x)$、$g(x)$相结合，mod$p$。

定义　若一n次多项式$f(x)$不能分解为两个低于n次的多项式的积，mod$p$，则此多项式称为对模p的不可化多项式，或对模p的素多项式。

定理15　任一多项式必可分解为不可化多项式的积，mod$p$；舍结合关系及次序外，此分解法是唯一的。

定理16　有二多项式$m(x)$及$n(x)$，使

$$m(x) f(x) + n(x) g(x) \equiv (f(x),\ g(x)) \pmod{p}.$$

定义　若一多项式$f(x)$能被另一个非常数的多项式的平方整除，mod$p$，则称$f(x)$有重因子，mod$p$。

定理17　$f(x)$有重因子的充分必要条件是

$$\partial^{\circ}\{(f(x),\ f'(x))\}\geqslant 1.$$

定理18　若$t\nmid n$，则$x^{n}-1$无重因子，mod$p$.

定理19　命 $(m,\ n)=d$，则

$$(x^m-1,\ x^n-1)=x^d-1.$$

定理20　命 $(m,\ n)=d$，则

$$(x^{p^m-1}-1,\ x^{p^n-1}-1)=x^{p^d-1}-1.$$

定义　命p表一素数，$\varphi(x)$为一多项式．若$f_1(x)-f_2(x)$为$\varphi(x)$之倍式，mod$p$，则称f_1及f_2对重模p、$\varphi(x)$同余，记为

$$f_1(x)\equiv f_2(x)\ (\mathrm{modd}\,p,\ \varphi(x)).$$

定理21　设$\varphi(x)$对p的次数为n．任一多项式必与下列多项式

$$a_1+a_2x+\cdots+a_nx^{n-1},\quad 0\leqslant a_i\leqslant p-1$$

之一同余，modd$p$，$\varphi(x)$．

定义　$a_1+\cdots+a_nx^{n-1}$，$0\leqslant a_i\leqslant p-1$所表出的$p^n$个多项式，称为重模$p$，$\varphi(x)$的一个完全剩余系；一完全剩余系中除去与$\varphi(x)$不互素的的，称为重模$p$，$\varphi(x)$的缩系．

定理22　设$\varphi(x)$为n次不可化多项式，mod$p$，则对任一非$\varphi(x)$倍式的多项式$f(x)$，mod$p$，恒有

$$(f(x))^{p^n-1}\equiv 1\ (\mathrm{mod}\,p,\ \varphi(x)).$$

对任一多项式常有

$$(f(x))^{p^n}\equiv f(x)\ (\mathrm{modd}\,p,\ \varphi(x)).$$

特别有

$$x^{p^n}\equiv x\ (\mathrm{modd}\,p,\ \varphi(x)).$$

定理23　任一n次不可化多项式一定整除$x^{p^n-1}-1$，mod p．

定理24　重模方程

$$f(X)\equiv 0\ (\mathrm{modd}\,p,\ \varphi(x))$$

的根的个数，不超过$f(X)$的次数。

定理25 $x^{p^n-1}-1$不被高于n次的不可化多项式所整除，mod$p$。

定理26 若$\psi(x)$为l次不可化多项式，mod$p$，且$\psi(x)\mid x^{p^n}-x \pmod p$，则$l\mid n$。

定理27 所有n次不可化多项式，mod$p$，其积等于

$$\frac{x^{p^n}-x}{\prod\limits_{q_1}(x^{p^{n/q_1}}-x)}\cdot\frac{\prod\limits_{q_1,q_2}(x^{p^{n/q_1q_2}}-x)}{\prod\limits_{q_1,q_2,q_3}(x^{p^{n/q_1q_2q_3}}-x)}\cdots \pmod p$$

此处q_1，$q_2\cdots$，过n的不同素因子。

定理28 共有

$$\frac{1}{n}\left(p^n-\sum_{q_1}p^{n/q_1}+\sum_{q_1,q_2}p^{n/q_1q_2}-\sum_{q_1,q_2,q_3}p^{n/q_1q_2q_3}+\cdots\right)$$

个n次不可化多项式，mod$p$。

定理29 必有一n次不可化多项式存在。

定义 设$(f(x),\ \varphi(x))=1$，若有一多项式$g(x)$使

$$(g(x))^m\equiv f(x)(\mathrm{modd}\,p,\ \varphi(x))\cdot$$

则$f(x)$名为m次剩余，modd$p$，$\varphi(x)$。

定义 若l是使

$$(f(x))^l\equiv 1\ (\mathrm{modd}\,p,\ \varphi(x))$$

成立的最小正整数，则称l为$f(x)$的次数。

定义 如果$f(x)$的次数$l=p^n-1$，则$f(x)$名为原根，modd$p$，$\varphi(x)$。

二、题　　解

§2　唯一分解定理

习题1　由第一章之内容试拟若干习题．

解：下面把第一章§1至§7中有关整数的一些性质（包括定理和习题）依次序推广到有理系数多项式集合上．这种推广，有些在本章§1和2中可以找到．但是为了便于和第一章§1至§7中有关整数的一些性质相互对照、比较，因而在这里仍把它们写出．这种从整数集合到有理系数多项式集合的推广，由下面的习题给出．它们的证明，与整数情形相同，故此处从略．而习题中的所有字母，如无特别声明，则均表示以x为变元的有理系数多项式．

练习1　任给二多项式f及g，g不恒为零，则必有二多项式g及r，使

$$f=qg+r,\text{ 此处}r=0\text{ 或}\partial^\circ r<\partial^\circ g.$$

练习2　若$b\neq 0$，$c\neq 0$，则

i)若$b|a$，$c|b$，则$c|a$；

ii)若$b|a$，则$bc|ac$；

iii)若$c|d$，$c|e$，则对任意多项式m、n，有

$$c|dm+en.$$

练习3　若b是a的真因式，则

$$1\leqslant\partial^\circ b<\partial^\circ a.$$

练习4　非常数的多项式都可以分解为素多项式的乘积．

练习5　任给二多项式a及b，则所有形如$am+bn$的多项式成一模．此处模定义为：对加、减自封的一多项式集合．

练习 6　证明：形如$am+bn$的多项式所成的模，由 (a, b) 的诸倍式组成。

练习 7　多项式 (a, b) 有如下性质：

i)有二多项式m，n，使 $(a, b)=am+bn$；

ii)对任二多项式m，n，必有 $(a, b)\mid am+bn$；

iii)若$e\mid a$，$e\mid b$，则$e\mid (a, b)$。

练习 8　若p为素多项式且$p\mid ab$，则

$$p\mid a \text{或} p\mid b.$$

练习 9　证明：如果c是首 1 多项式，则

$$c(a, b)=(ca, cb).$$

练习10　任一多项式都可分解为不可化多项式的积，若互相结合的多项式算作相同，并不计因式顺序，则此种分解法是唯一的。

练习11　命f及g都是首 1 多项式：

$$f=p_1^{a_1}\cdots p_s^{a_s},\ a_\nu \text{是非负整数；}$$

$$g=p_1^{b_1}\cdots p_s^{b_s},\ b_\nu \text{是非负整数.}$$

式中p_r是不相等的、不可化的首 1 多项式，则

$$(f, g)=p_1^{c_1}\cdots p_s^{c_s},\ \text{此处} c_\nu=\min(a_\nu, b_\nu).$$

练习12　如练习11的假定，可得

$$[f, g]=p_1^{d_1}\cdots p_s^{d_s},\ \text{此处} d_\nu=\max(a_\nu, b_\nu).$$

练习13　证明：二多项式a、b的任一公倍式必是它们最小公倍式的倍式。

练习14　证明：若a、b是首 1 多项式，则

$$ab=[a, b]\cdot(a, b).$$

用归纳法定义多个多项式的最大公因式及最小公倍式：

$$(a_1, \cdots, a_n)=((a_1, \cdots, a_{n-1}), a_n);$$

$$[a_1, \cdots, a_n]=[[a_1, \cdots, a_{n-1}], a_n].$$

练习15　命

$$a_1=p_1^{e_{11}}\cdots p_s^{e_{1s}},\quad \cdots,\quad a_n=p_1^{e_{n1}}\cdots p_s^{e_{ns}};$$

其中a_ν是首1多项式，p_ν是不相等的、不可化的首1多项式，$e_{\lambda\nu}$是非负整数，则

$$(a_1,\ \cdots,\ a_n)=p_1^{e_1}\cdots p_s^{e_s},\quad e_\nu=\min(e_{1\nu},\ \cdots,\ e_{n\nu});$$

$$[a_1,\ \cdots,\ a_n]=p_1^{d_1}\cdots p_s^{d_s},\quad d_\nu=\max(e_{1\nu},\ \cdots,\ e_{n\nu}).$$

练习16　证明下列二式：

$$(a_1,\ \cdots,\ a_n)=((a_1,\ \cdots,\ a_s),\ (a_{s+1},\ \cdots,\ a_n));$$

$$[b_1,\ \cdots,\ b_n]=[[b_1,\ \cdots,\ b_s],[b_{s+1},\cdots,\ b_n]].$$

练习17　若a_1，…，a_n都是首1多项式，则

$$(a_1,\ \cdots,\ a_n)=\frac{a_1\cdots a_n}{[a_2\cdots a_n,a_1a_3\cdots a_n,\ \cdots,a_1\cdots a_{n-1}]},$$

$$[b_1,\ \cdots,\ b_n]=\frac{a_1\cdots a_n}{(a_2\cdots a_n,\ a_1a_3\cdots a_n,\ \cdots,\ a_1\cdots a_{n-1})}.$$

练习18　证明：多项式（a_1，…，a_n）是形如

$$a_1m_1+\cdots\cdots a_nm_n$$

诸多项式中次数最低的一个。

练习19　若a_1，…，a_n都是首1多项式，则

$$[a_1,\ \cdots,\ a_n]=a_1\cdots a_n(a_1,\ a_2)^{-1}\cdots(a_{n-1},\ a_n)^{-1}$$
$$(a_1,\ a_2,\ a_3)\cdots(a_1,\ \cdots,\ a_n)^{(-1)^{n+1}}.$$

练习20　如练习19的假定，则

$$(a_1,\ \cdots,\ a_n)=a_1\cdots a_n[a_1,\ a_2]^{-1}\cdots[a_{n-1},\ a_n]^{-1}$$
$$[a_1,\ a_2,\ a_3]\cdots[a_1,\ \cdots,\ a_n]^{(-1)^{n+1}}.$$

习题2　试将理想集合的观念推广到含多个变数的多项式，并举例证明定理1、2并不真实。

解：设I是一n元（$n\geq 2$）多项式所成的集合，如果适合以下条件，则称I是一个理想集合：

i）若f、g为I中的多项式，则$f+g$也是I中的多项式；

ii)若f在I中，h为任一n元多项式，则hf也在I中。

定理1.2指出：任一理想集合中可以找到一多项式f，使凡此集合中的多项式皆为f的倍式，即是说该集合由f的所有倍式组成。

设I为形如$mf+ng$的多项式所成的理想集合，其中

$$f=x^2+y^2,\qquad g=x^2-y^2$$

而m、n为关于x、y的任意二元多项式。如果I中有一多项式d，使得I中任意多项式都是d的倍式，那么就有$d|x^2+y^2$。又因x^2+y^2不可化，因此$d=1$或者x^2+y^2。$d=x^2+y^2$给出$x^2+y^2|x^2-y^2$，此不可能，故$d=1$。这就是说，I包有所有关于x、y的二元多项式。因此对于$x+y$，可找到多项式$m_1(x,y)$、$n_1(x,y)$，使得

$$x+y=m_1(x,y)(x^2+y^2)+n_1(x,y)(x^2-y^2)$$

显然$x+y|m_1(x,y)$，若设$m_1(x,y)=m_1'(x,y)(x+y)$，则

$$1=m_1'(x,y)(x^2+y^2)+n_1(x,y)(x-y),$$

此乃一恒等式，取$y=x$就有

$$1=m_1'(x,x)2x^2,$$

从而有　$x^2|1$，

此不可能。因此定理1.2在多元理想中并不真实。

§3　同余式

习题1　设α_1、α_2、α_3各不相同。求一二次多项式$f(x)$适合于

$$f(\alpha_1)=\beta_1,\ f(\alpha_2)=\beta_2,\ f(\alpha_3)=\beta_3$$

并说明其与大衍求一术之关系。

解：我们将证明

$$F(x)=\beta_1\frac{(x-a_2)(x-a_3)}{(a_1-a_2)(a_1-a_3)}+\beta_2\frac{(x-a_3)(x-a_1)}{(a_2-a_3)(a_2-a_1)}$$
$$+\beta_3\frac{(x-a_1)(x-a_2)}{(a_3-a_1)(a_3-a_2)}$$

就是合条件的多项式．即证明$F(x)=f(x)$．

因为
$$f(a_1)=\beta_1=F(a_1)$$
$$f(a_2)=\beta_2=F(a_2)$$
$$f(a_3)=\beta_3=F(a_3)$$

并且$f(x)$、$F(x)$都是二次多项式，故有
$$F(x)=f(x)$$

与大衍求一术的关系如下：
$$f(a_1)=\beta_1，\ f(a_2)=\beta_2，\ f(a_3)=\beta_3$$
与　$x\equiv a_1(\mathrm{mod}m_1)$，$x\equiv a_2(\mathrm{mod}m_2)$，$x\equiv a_3(\mathrm{mod}m_3)$
相对应；β_1、β_2、β_3与a_1、a_2、a_3相对应；而a_1、a_2、a_3又与m_1、m_2、m_3相对应；a_1、a_2、a_3各不相同，与m_1、m_2、m_3两两互素相对应；最后，唯一的多项式$f(x)$与唯一解$x\equiv a(\mathrm{mod}m_1m_2m_3)$相对应．由此看来，此二法“面貌虽不同，原则本无隔”．

习题 2　设$m_1(x)$与$m_2(x)$为二不互相结合之不可化多项式．命$f_1(x)$及$f_2(x)$为所与之多项式．证明必有一多项式$f(x)$，使
$$f(x)\equiv f_1(x)(\mathrm{mod}m_1(x))$$
$$f(x)\equiv f_2(x)(\mathrm{mod}m_2(x))\ .$$

证：由于$m_1(x)$与$m_2(x)$既不相结合，又均不可化，故有$(m_1(x),\ m_2(x))=1$．因而，如果设
$$M_1(x)=m_2(x),\ M_2(x)=m_1(x)$$
就一定存在$M_1'(x)$、$M_2'(x)$，使得
$$M_1(x)M_1'(x)\equiv 1\ (\mathrm{mod}m_1(x))$$
$$M_2(x)M_2'(x)\equiv 1\ (\mathrm{mod}m_2(x))\ .$$

如果取 $f(x)\equiv M_1(x)M_1'(x)f_1(x)+M_2(x)M_2'(x)f_2(x)$

$(\mathrm{mod}\, m_1(x)m_2(x))$

就有 $f(x)\equiv f_1(x)(\mathrm{mod}\, m_1(x))$

$f(x)\equiv f_2(x)(\mathrm{mod}\, m_2(x))$.

习题 3 试推广以上二习题。

解： 先推广习题 1 的结论。设α_1, …, α_n , α_{n+1}各不相同，如果n次多项式$f(x)$适合

$$f(\alpha_1)=\beta_1,\ \cdots,\ f(\alpha_n)=\beta_n,\ f(\alpha_{n+1})=\beta_{n+1}$$

则
$$f(x)=\beta_1\frac{(x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_{n+1})}{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\cdots(\alpha_1-\alpha_{n+1})}$$

$$+\beta_2\frac{(x-\alpha_1)(x-\alpha_3)\cdots(x-\alpha_{n+1})}{(\alpha_2-\alpha_1)(\alpha_2-\alpha_3)\cdots(\alpha_2-\alpha_{n+1})}$$

$$+\cdots+\beta_{n+1}\frac{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)}{(\alpha_{n+1}-\alpha_1)(\alpha_{n+1}-\alpha_2)\cdots(\alpha_{n+1}-\alpha_n)}$$

这就是lagrange插值公式。证法与习题 1 同。

再推广习题 2 的结论。设$m_1(x)$, …, $m_n(x)$为两两不互相结合的不可化多项式。命$f_1(x)$, …, $f_n(x)$为所给的多项式，则必有一多项式$f(x)$，使得

$$f(x)\equiv f_1(x)(\mathrm{mod}\, m_1(x))\ ,\ \cdots,\ f(x)\equiv f_n(x)(\mathrm{mod}\, m_n(x))$$

欲证此点，我们设

$$M(x)=m_1(x)\cdots m_n(x)=m_1(x)M_1(x)=\cdots=m_n(x)M_n(x)$$

因为 $(m_i(x),\ m_j(x))=1,\quad 1\leqslant i\neq j\leqslant n$

所以存在$M_1'(x)$, …, $M_n'(x)$，使得

$$M_1(x)M_1'(x)\equiv 1\ (\mathrm{mod}\, m_1(x))$$
$$M_2(x)M_2'(x)\equiv 1\ (\mathrm{mod}\, m_2(x))$$
$$\cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots$$
$$M_n(x)M_n'(x)\equiv 1\ (\mathrm{mod}\, m_n(x))$$

只要取

$$f(x)\equiv M_1(x)M_1'(x)f_1(x)+\cdots+M_n(x)M_n'(x)f_n(x) \pmod{M(x)}$$

就有

$$f(x)\equiv f_1(x)\pmod{m_1(x)},\cdots,\ f(x)\equiv f\ (x)\pmod{m_{\ }(x)}$$

§4 整系数多项式

习题 1　试将定理 1 推广到n个变数的情况。

解：定理 1 是关于一元整系数多项式所成理想的 Hilbert 定理，即在一理想集合A中必有有限多个整系数多项式f_1，…，f_n具有如下性质：A中任一多项式f必可表为

$$f=g_1f_1+\cdots+g_nf_n$$

此处g_1，…g_n，也是整系数多项式。

n个变数的情况与该定理 1 完全一样，只需把定理 1 应用n次便可证明，故此处从略。

定理 1 还可写成下面稍强的形式：

定理 1′　在一理想集合A中，必有l个整系数多项式f_1，…，f_l 和一整数D，使得A中任一多项式f必可表为

$$f=qf_1+c_2f_2+\cdots+c_lf_l+c_{l+1}D$$

其中q是整系数多项式，c_i（$2\leqslant i\leqslant l+1$）是整数，$\partial^\circ f_j=l-j$（$0\leqslant j\leqslant l-1$），而$l$是$A$中多项式的最高方次系数所成模的生成元所对应的多项式的次数。

证：1)′同定理 1 证明中的 1）。

2)′同定理 1 证明中的 2）。

3)′对A中次数$<l$的多项式中x^{l-1}的系数添加 0，作成集合B_1，易证B_1成一模。设B_1的生成元d_1所对应的多项式为

$$f_2(x)=d_1x^{l-1}+\cdots$$

对A中任何一个次数等于$l-1$的多项式

$$f(x)=ax^{l-1}+\cdots$$

由于$d_1|a$，故

$$f(x)-\frac{a}{d_1}f_2(x)$$

是一个次数$<l-1$的整系数多项式。也就是说，存在整数c_2和整系数多项式$r(x)$，使得

$$f(x)=c_2f_2(x)+r(x)$$

此处$\partial^\circ r<l-1$或$r=0$。类似地，对A中所有次数$<l-1$的多项式中x^{l-2}的系数添加0，作成模B_2，设B_2的生成元d_2对应的多项式为

$$f_3(x)=d_2x^{l-2}+\cdots$$

那么A中任何一个次数等于$l-2$的多项式$f(x)$都可以写成

$$f(x)=c_3f_3(x)+r(x)$$

此处$\partial^\circ r<l-2$或$r=0$。继续使用此法，便可得到定理1′。

习题2　试将定理1中之整系数多项式换为整值多项式而研究其正确性。

解：如果把定理1中的整系数多项式换为整值多项式，那么结论就不一定成立。为证此点，先证明下面一个引理。

引理　整值多项式所成理想A存在有限基的充分必要条件是A中存在有限多个整值多项式f_1，…，f_n，使A中任一整值多项式F总满足

$$\partial^\circ F\geqslant\partial^\circ(F-g_1f_1)\geqslant\cdots\geqslant\partial^\circ(F-g_1f_1-\cdots g_nf_n)=0$$

其中g_1…，g_n也是整值多项式。

先证充分性。

因为　　$\partial^\circ(F-g_1f_1-\cdots-g\ f\ )=0$

所以　　$F=g_1f_1+g\ f_n+a$

式中a为整数。易证A中诸整数连同零成为一模。设此模的生成元为f_{n+1}，从而$a=g_{n+1}f_{n+1}$，由于g_{n+1}为整数，故

$$F = g_1 f_1 + \cdots + g_n f_n + g_{n+1} f_{n+1}$$

此即A存在有限基。

再证必要性。设f_1，…，f_n是A的一组有限基，则A中任一整值多项式F都可表示成

$$F = g_1 f_1 + \cdots + g_n f_n$$

其中g_1，…，g_n都是整值多项式。

不失一般，设

$$\partial^\circ(g_1 f_1) \geqslant \partial^\circ(g_2 f_2) \geqslant \cdots \geqslant \partial^\circ(g_n f_n)$$

如果取$\partial^\circ(0) = 0$，则

$$\partial^\circ F \geqslant \partial^\circ(F - g_1 f_1) \geqslant \cdots \geqslant \partial^\circ(F - g_1 f_1 - \cdots g_n f_n) = 0$$

必要性由此得证。

A中诸整值多项式的首项系数成一集合B，此B是一个域。设若

$$F(x) = \frac{b}{a}x^n + \cdots,\quad \Phi(x) = \frac{d}{c}x^m + \cdots$$

是A中二整值多项式，$\frac{b}{a}$、$\frac{d}{c}$是既约分数，那么，由理想的定义可知

$$x^m F \pm x^n \Phi = \left(\frac{b}{a} \pm \frac{d}{c}\right) x^{n+m} + \cdots$$

$$F \cdot \Phi = \frac{b}{a} \cdot \frac{d}{c} x^{n+m} + \cdots$$

均在A中，即有$\frac{b}{a} \pm \frac{d}{c} \in B$，$\frac{b}{a} \cdot \frac{d}{c} \in B$。又因

$$H(x) = c^2 \binom{x}{d^2} = \frac{c^2}{d^2!} x^{d^2} + \cdots$$

是整值多项式，故$(d^2 - 1)!\,H(x)$是整值多项式，因此

$$(d^2 - 1)!\,HF\Phi = \frac{b}{a} \Big/ \frac{d}{c} x^{n+m+d^2} + \cdots$$

仍在A中，即有 $\frac{b}{a}\Big/\frac{d}{c}\in B$，所以$B$成一域，从而$B$只含主理想$(0)$，$(1)$。因此$A$中必含有首1多项式。

设 $f_1(x)=x^l+\cdots$

是A中一个首1多项式，对A中任一整值多项式

$$F(x)=\frac{b}{a}x^n+\cdots,$$

当$n\geqslant l$时，虽然

$$F-\left(\frac{b}{a}x^{n-l}+\alpha_1x^{n-l-1}+\cdots+\alpha_{n-l}\right)f_1$$

是一个次数$\leqslant n-1$的多项式，但是

$$g(x)=\frac{b}{a}x^{n-l}+\cdots+\alpha_{n-l}$$

不一定是整值多项式。例如，$n-l=1$时，$g(x)=\frac{b}{a}x+\alpha_1=\frac{b}{a}\binom{x}{1}+\alpha_1$。由第一章提要中定理26可知，$g(x)$为整值多项式的条件是$\frac{b}{a}$和$\alpha_1$都必须是整数，因此$F-gf_1$不一定在$A$中。实际上，任意取定$A$中一个整值多项式

$$f_1'(x)=\frac{d'}{c'}x^{l'}+\cdots$$

当$n\geqslant l'$时，虽然

$$\partial^\circ F>\partial^\circ\left[F-\left(\frac{bc'}{ad'}x^{n-l'}+\beta_1x^{n-l'-1}+\cdots+\beta_{n-l'}\right)f_1'\right]$$

但是同样也不能断定

$$g'(x)=\frac{bc'}{ad'}x^{n-l'}+\cdots+\beta_{n-l'}$$

是整值多项式，因此$F-g'f_1'$不一定在A中。这也就是说，整值多项式所成的理想A条件

$$\partial^\circ F\geqslant\partial^\circ(F-g_1f_1)\geqslant\cdots\geqslant\partial^\circ(F-g_1f_1-\cdots-g f)=0$$

不一定被满足。故由引理可知，A不一定存在有限基，即如果把定理1中的整系数多项式换为整值多项式后，结论就不一定成立。

§7 重模同余式

习题 试推广Euler函数之定义。进而求出其表示公式。

解：设$\varphi(x)$对素数p的次数为n，任一多项式必与下列多项式之一

$$a_1+a_2x+\cdots+a_nx^{n-1},\quad 0\leqslant a_i\leqslant p-1 \qquad (1)$$

同余，显然(1)表p^n个多项式，其中任何两个对重模p、$\varphi(x)$都不同余，且任一多项式必与(1)中某一个同余moddp，$\varphi(x)$。由(1)所表出的p^n个多项式称为重模moddp，$\varphi(x)$的完全剩余系，其中与$\varphi(x)$互素者构成重模moddp，$\varphi(x)$的缩系。现将Euler函数的定义作如下推广：命$\Phi(p,\varphi(x))$表重模p，$\varphi(x)$的缩系所含多项式的个数，可以得到如下两个定理。

定理1 当$\varphi(x)$为n次不可化时，mod$p$，则

$$\Phi(p,\ \varphi(x))=p^n-1 \qquad (2)$$

证：i)如果$\varphi(x)$不可化，mod$p$，则$\varphi(x)$原来也不可化。否则，设$\varphi(x)=h(x)\varphi)(x)$，就有

$$\varphi(x)\equiv h(x)\varphi'(x)(\text{mod}p)$$

这与$\varphi(x)$为不可化，mod$p$相矛盾。

ii)如果$\varphi(x)$不可化，mod$p$，由i)知$\varphi(x)$原来不可化，此时若$\varphi(x)$与$a_1+a_2x+\cdots+a_nx^{n-1}$不互素（其中$a$不全为0），则由提要中定理6就有

$$\varphi(x) \mid a_1 + a_2 x + \cdots + a_n x^{n-1}$$

但$\partial^\circ\varphi \geqslant n$，故此不可能．由i)ii)可知，（1）中所表的$p^n$个多项式，除去0外都与$\varphi(x)$互素，故

$$\Phi(p,\ \varphi(x)) = p^n - 1$$

定理 2　当$\varphi(x) \equiv \prod_{i=1}^{k} \varphi_i(x) \pmod{p}$，其中$\varphi_i(x)$为$\alpha_i$次不可化多项式，mod$p$，且$\sum_{i=1}^{k}\alpha_i = n$时，

$$\Phi(p,\ \varphi(x)) = p^n \prod_{i=1}^{k} \left(1 - \frac{1}{p^{\alpha_i}}\right) \tag{3}$$

证： 如果$\varphi_1(x)$，$\cdots$，$\varphi_k(x)$都与$a_1 + a_2 x + \cdots + a_n x^{n-1}$互素，则$\prod_{i=1}^{k}\varphi_i(x)$也与它互素，故由定理1得

$$\Phi(p,\ \varphi(x)) = \prod_{i=1}^{k} \Phi(p,\ \varphi(x)) = \prod_{i=1}^{k} (p^{\alpha_i} - 1)$$

注意到$\sum_{i=1}^{k}\alpha_i = n$，立得

$$\Phi(p,\ \varphi(x)) = p^n \prod_{i=1}^{k} p^{-\alpha_i} \prod_{i=1}^{k} (p^{\alpha_i} - 1)$$

$$= p^n \prod_{i=1}^{k} \left(1 - \frac{1}{p^{\alpha_i}}\right).$$

显然，（2）是一般Euler函数$\varphi(p) = p - 1$的推广，而（3）则是一般Euler函数$\varphi(m) = m\prod_{p|m}\left(1 - \frac{1}{p}\right)$的推广。

§ 8 Fermat定理之推广

习题 试推广第二章中之 Euler 定理。

解：命$f_1(x)$，$f_2(x)$，…，$f_{\Phi(p,\varphi(x))}(x)$
为一缩系，moddp，$\varphi(x)$。由于$f(x)$为任一与$\varphi(x)$互素的多项式，因此

$$f(x)f_1(x), \cdots, f(x)f_{\Phi(p,\varphi(x))}(x)$$

也为一缩系，moddp,$\varphi(x)$，故

$$\prod_{i=1}^{\Phi(p,\varphi(x))} f_i(x) \equiv \prod_{i=1}^{\Phi(p,\varphi(x))} (f(x)f_i(x))(\operatorname{modd}p,\ \varphi(x))$$

即

$$\left((f(x))^{\Phi(p,\varphi(x))}-1\right)\prod_{i=1}^{\Phi(p,\varphi(x))} f_i(x)$$
$$\equiv 0\ (\operatorname{modd}p,\ \varphi(x))$$

又因为 $\prod_{i=1}^{\Phi(p,\varphi(x))} f_i(x)$与$\varphi(x)$互素，故有

$$(f(x))^{\Phi(p,\varphi(x))} \equiv 1\ (\operatorname{modd}p,\ \varphi(x))$$

此即推广的Euler定理。

习题 设$\psi(x)$及$\varphi(x)$都是不可化多项式，mod$p$，则

$$\psi(X) \equiv 0\ (\operatorname{modd}p,\ \varphi(x))$$

可解之必要且充分之条件为$\partial°\psi|\partial°\varphi$。并证若可解则可分解为一次因子之积。

证：设$\partial°\psi=m$，$\partial°\varphi=n$。由题要中定理22知，对任一多项式X恒有

$$X^{p^n}-X\equiv 0\ (\operatorname{modd}p,\ \varphi(x)) \qquad (1)$$

而下面的p^n 个多项式

$$a_i=a_{i1}+a_{i2}x+\cdots+a_{in}x^{n-1}$$

其中 $0\leqslant a_{ij}\leqslant p-1$， $1\leqslant i\leqslant p^n$ ， $1\leqslant j\leqslant n$
构成重模p，$\varphi(x)$的完全剩余系，故

$$X^{p^n}-X\equiv(X-\alpha_1)\ \cdots\ (X-\alpha_{p^n})(\mathrm{modd}\,p,\ \varphi(x))$$

先证必要性。

若

$$\psi(X)\equiv 0\ (\mathrm{modd}\,p,\ \varphi(x)) \qquad (2)$$

可解，那么由前述知道（2）必与（1）有公共解．设

$$X\equiv g(x)(\mathrm{modd}\,p,\ \varphi(x))$$

为一公共解，则

$$\psi(X)\equiv(X-g(x))H_1(X)(\mathrm{modd}\,p,\ \varphi(x)) \qquad (3)$$

$$X^{p^n}-X\equiv(X-g(x))H_2(X)(\mathrm{modd}\,p,\ \varphi(x)) \qquad (4)$$

如果 $(\psi(X),X^{p^n}-X)\equiv 1\ (\mathrm{mod}\,p)$

注意到 $(\psi(X),\ X^{p^n}-X)\equiv(\psi(X),\ X^{p^n}-X)(\mathrm{mod}\,\varphi(x))$

立刻可以推出 $(\psi(X),\ X^{p^n}-X)\equiv 1\ (\mathrm{modd}\,p,\ \varphi(x))$
这就和（3）、（4）矛盾．因此

$$(\psi(X),\ X^{p^n}-X)\equiv 1\ (\mathrm{mod}\,p)$$

不成立；结合已知$\psi(X)$关于X不可化，mod$p$，可得

$$\psi(X)\mid X^{p^n}-X(\mathrm{mod}\,p)$$

再由定理26得$m\mid n$。

再证充分性。

由 $\psi(x)\mid x^{p^m}-x(\mathrm{mod}\,p)$

和定理20 $(x^{p^n}-x,\ x^{p^m}-x)=x^{p^m}-x$

可得 $\psi(x)\mid x^{p^n}-x(\mathrm{mod}\,p)$

$$\psi(X)\mid X^{p^n}-X(\mathrm{mod}\,p)$$

所以 $X^{p^n}-X\equiv\psi(X)H(X)(\mathrm{mod}\,p)$

$$X^{p^n}-X\equiv\psi(X)H(X)(\mathrm{modd}\,p,\ \varphi(x))$$

$$(X-\alpha_1)\ \cdots\ (X-\alpha_{p^n})\equiv\psi(X)H(X)(\mathrm{modd}\,p,\ \varphi(x)) \qquad (5)$$

因为 $\partial^\circ H=p^n-m$， $m\geqslant 1$，故若（2）不可解，则由（5）就得出，

$H(X)\equiv 0\ (\mathrm{modd}p,\ \varphi(x))$ 的解数是p^n，而$p^n>p^n-m=\partial^\circ H$，与定理24相矛盾，因此（2）一定可解。又因为$a_1$，…，$a_{p^n}$是重模$p$，$\varphi(x)$的一完全剩余系，故

$$\psi(X)\equiv(X-\beta_1)\cdots(X-\beta_k)(\mathrm{modd}p,\ \varphi(x)) \qquad (2')$$

其中β_1，…，β_k从a_1，…，a_{p^n}中取出。这就证明了充分性，并且也证明了（2）若可解则可分解为一次因子的积。

（2′）中$k=m$，若不然，则由定理24就有$k<m$，再由（5）推出重模方程

$$H(X)\equiv 0\ (\mathrm{modd}p,\ \varphi(x))$$

的解数$p^n-k>p^n-m$，与$\partial^\circ H=p^n-m$矛盾。

§9　对模p之不可化多项式

习题　无遗漏地补出下一节中所略去的证明。

解：仿照第三章中关于整数性质的几个定理，容易给出下面五个定理的证明。

定理1　$f(x)$是二次剩余$\mathrm{modd}p$，$\varphi(x)$的充分必要条件为

$$(f(x))^{\frac{1}{2}(p^n-1)}\equiv 1\ (\mathrm{modd}p,\ \varphi(x))$$

不然则为

$$(f(x))^{\frac{1}{2}(p^n-1)}\equiv -1\ (\mathrm{modd}p,\ \varphi(x))$$

其中p表奇素数，$\varphi(x)$是n次不可化，$\mathrm{mod}p$。

证：i)若$f(x)$是二次剩余$\mathrm{modd}p$，$\varphi(x)$，那么存在$g(x)$，使得

$$(g(x))^2\equiv f(x)(\mathrm{modd}p,\ \varphi(x))$$

从而

$$(f(x))^{\frac{1}{2}(p^n-1)}\equiv(g(x))^{p^n-1}\equiv 1\ (\mathrm{modd}p,\varphi(x))$$

必要性由此得证。再证充分性。在重模p，$\varphi(x)$缩系中的k次

多项式($k=0,1,\cdots,n-1$)首项系数为 $1,2,\cdots,\frac{1}{2}(p-1)$ 的共有

$$\sum_{k=0}^{n-1}\left(\frac{p-1}{2}\right)p^k=\frac{p-1}{2}\cdot\frac{p^n-1}{p-1}=\frac{1}{2}(p^n-1)$$

个，记为 $\quad f_1(x),\ f_2(x),\ \cdots,f_{\frac{1}{2}(p^n-1)}(x)$。

现在证明

$$f_1^2(x),\ f_2^2(x),\ \cdots,\ f^2_{\frac{1}{2}(p^n-1)}(x) \qquad (1)$$

给出重模$p,\varphi(x)$的全部二次剩余。设$f(x)$是一个二次剩余modd$p$, $\varphi(x)$，则存在$g(x)$，使得

$$f(x)\equiv(g(x))^2\equiv(-g(x))^2(\mathrm{modd}p,\ \varphi(x))\ .$$

如果$g(x)$的首项系数在1和$\frac{1}{2}(p-1)$之间，则 $(g(x))^2$在(1)中，如果$g(x)$的首项系数大于$\frac{1}{2}(p-1)$，则 $(-g(x))$的首项系数在1和$\frac{1}{2}(p-1)$之间，因此 $(-g(x))^2$ 在(1)中。所以$f(x)$必与(1)中某一个同余。(1)中任何两个都不同余，否则有

$$f_i^2(x)\equiv f_j^2(x)(\mathrm{modd}p,\ \varphi(x)),\ 1\leqslant i<j\leqslant\frac{1}{2}(p^n-1)$$

即 $\qquad \varphi(x)\mid(f_i(x)-f_j(x))(f_i(x)+f_j(x))(\mathrm{mod}p)$

再由$\varphi(x)$为$-n$次不可化多项式，mod$p$可得

$$\varphi(x)\mid f_i(x)-f_j(x)(\mathrm{mod}p)$$

或 $\qquad \varphi(x)\mid f_i(x)+f_j(x)(\mathrm{mod}p)$.

如果 $\qquad \varphi(x)\mid f_i(x)-f_j(x)(\mathrm{mod}p)$

成立，即是说$f_i(x)\equiv f_j(x)\ (\mathrm{modd}\,p,\ \varphi(x))$成立，此与前设$f_i(x)$，$f_j(x)$都在缩系中矛盾。若有

$$\varphi(x)\,|\,f_i(x)+f_j(x)\ (\mathrm{mod}\,p)$$

则存在$m(x)$，使得

$$f_i(x)+f_j(x)\equiv m(x)\varphi(x)\ (\mathrm{mod}\,p)$$

但是$\partial^\circ f_i<\partial^\circ\varphi$，$\partial^\circ f_j<\partial^\circ\varphi$，因此

$$m(x)\equiv 0\ (\mathrm{mod}\,p)$$

故
$$f_i(x)+f_j(x)\equiv 0\ (\mathrm{mod}\,p)\ . \qquad (2)$$

若用a_i，a_j分别记f_i和f_j的首项系数，那么当$\partial^\circ f_i>\partial^\circ f_j$或$\partial^\circ f_i<\partial^\circ f_j$或$\partial^\circ f_i=\partial^\circ f_j$时，(2)分别给立$p|a_i$或$p|a_j$或$p|a_i+a_j$但此三种情形都与

$$1\leqslant a_i\leqslant\frac{1}{2}(p-1)\ ,\qquad 1\leqslant a_j\leqslant\frac{1}{2}(p-1)$$

相矛盾。故(1)中任何两个都不同余。

另一方面，由提要中定理24可知同余方程

$$X^{\frac{1}{2}(p^n-1)}\equiv 1\ (\mathrm{modd}\,p,\ \varphi(x)) \qquad (3)$$

的解数$\leqslant\frac{1}{2}(p^n-1)$，因此(1)给出(3)的全部解。故若

$$(f(x))^{\frac{1}{2}(p^n-1)}\equiv 1\ (\mathrm{modd}\,p,\ \varphi(x))$$

则$f(x)$定是一个二次剩余moddp，$\varphi(x)$。充分性由此得证。

ii)因为

$$\varphi(x)\,\Big|\,\Big((f(x))^{\frac{1}{2}(p^n-1)}-1\Big)\cdot\Big((f(x))^{\frac{1}{2}(p^n-1)}+1\Big)\ (\mathrm{mod}\,p)$$

故若

$$\varphi(x)\nmid(f(x))^{\frac{1}{2}(p^n-1)}-1\ (\mathrm{mod}\,p)\ ,$$

则一定有 $\varphi(x) \mid (f(x))^{\frac{1}{2}(p^n-1)}+1 \pmod p$，

即 $(f(x))^{\frac{1}{2}(p^n-1)} \equiv -1 \,(\text{modd}\, p,\ \varphi(x))$.

定理 2 若$f(x)$对重模p，$\varphi(x)$的次数为l，则$l \mid p^n-1$。

证：如果$l \nmid p^n-1$，可设$p^n-1=ql+r$，$1 \leqslant r \leqslant l-1$。因为

$$(f(x))^{p^n-1} \equiv (f(x))^{ql+r} \equiv [(f(x))^l]^q \cdot (f(x))^r \,(\text{modd}\, p,\ \varphi(x))$$

且 $(f(x))^{p^n-1} \equiv (f(x))^l \equiv 1 \,(\text{modd}\, p,\ \varphi(x))$

故有 $(f(x))^r \equiv 1 \,(\text{modd}\, p,\ \varphi(x))$，这与$l$最小矛盾，故

$$l \mid p^n-1.$$

定理 3 次数为l的互不同余的多项式的个数为$\Phi(l)$，此处$\Phi(l)$为Euler函数。

证：先证$\Phi(l)$的若干性质，再证$\Phi(l)$就是Euler函数。

i)若 $(l_1,\ l_2)=1$，则$\Phi(l_1 l_2)=\Phi(l_1)\Phi(l_2)$。命$h_1(x)$，$h_2(x)$的次数为$l_1$、$l_2$，$h_1(x)h_2(x)$的次数为$l$，则

$$1 \equiv (h_1(x)h_2(x))^{ll_2} \equiv (h_1(x))^{ll_2} \,(\text{modd}\, p,\ \varphi(x))$$

由定理2得，$l_1 \mid ll_2$。但 $(l_1,\ l_2)=1$，故$l_1 \mid l$。同法$l_2 \mid l$，故$l=l_1 l_2$，即$h_1(x)h_2(x)$的次数为$l_1 l_2$。所以，如有一多项式$h_1(x)$其次数为l_1，另一多项式$h_2(x)$其次数为l_2，则可做出一多项式$h_1(x)h_2(x)$，其次数为$l_1 l_2$。今证：

若非 $h_1(x) \equiv h_1'(x)$，$h_2(x) \equiv h_2'(x) \,(\text{modd}\, p,\ \varphi(x))$

则 $h_1(x)h_2(x) \equiv h_1'(x)h_2'(x) \,(\text{modd}\, p,\ \varphi(x))$

不成立。这是因为，如果

$$h_1(x)h_2(x) \equiv h_1'(x)h_2'(x) \,(\text{modd}\, p, \varphi(x))$$

则

$$h_1(x)h_1'(x)^{-1} \equiv h_2(x)^{-1}h_2'(x) \,(\text{modd}\, p, \varphi(x))$$

但$h_1(x)h_1'(x)^{-1}$的次数$\mid l_1$，$h_2'(x)h_2(x)^{-1}$的次数$\mid l_2$，故必有

$$h_1(x)h_1'(x)^{-1}\equiv h_2'(x)h_2(x)^{-1}\equiv 1\ (\mathrm{modd}\,p,\ \varphi(x))$$

而这与假设矛盾。反之，若有一多项式$h(x)$，其次数是l_1l_2，$(l_1, l_2)=1$，则有$h_1(x)=h(x)^{l_2}$，$h_2(x)=h(x)^{l_1}$，其次数各为l_1、l_2，故得

$$\Phi(l_1)\Phi(l_2)=\Phi(l_1l_2)$$

ii)设$l=q^t$，q为素数，则由§8习题知道

$X^{q^t}-1\equiv 0\ (\mathrm{modd}\,p,\ \varphi(x))$ 的解数为q^t，若X适合此式而次数非q^t，则必适合

$$X^{q^{t-1}}-1\equiv 0\ (\mathrm{modd}\,p,\ \varphi(x))$$

此式的解数为q^{t-1}，故

$$\Phi(q^t)=q^t-q^{t-1}.$$

由i)、ii)便知$\Phi(l)$为Euler函数。

定理 4 若$f(x)$是一原根，则$(f(x))^{\nu}$，$\nu=1, 2, \cdots, p^n-1$表示所有非零的、互不同余的多项式（$\mathrm{modd}\,p,\ \varphi(x)$）.

证：若有正整数r、s，$1\leqslant r<s\leqslant p^n-1$，使得

$$(f(x))^s\equiv(f(x))^r\ (\mathrm{modd}\,p,\ \varphi(x))$$

成立，那么就有

$$(f(x))^{s-r}\equiv 1\ (\mathrm{modd}\,p,\varphi(x))$$

由于$f(x)$是原根，不可能推出$p^n-1\,|\,s-r$。

定理 5

$$\prod_{\nu}(X-f_\nu(x))\equiv\frac{X^{p^n}-1}{\prod_q\left(X^{(p^n-1)/q}-1\right)}\cdot$$

$$\frac{\prod_{q,q_1}\left(X^{(p^n-1)/qq_1}-1\right)}{\prod_{q,q_1,q_2}\left(X^{(p^n-1)/qq_1q_2}-1\right)}\cdots\ (\mathrm{modd}\,p,\ \varphi(x)).$$

此处$f_\nu(x)$过所有原根，$\prod\limits_{q}$过p^n-1的所有素因子q，$\prod\limits_{q,q_1}$过p^n-1的所有素因子对q、q_1，且$q\neq q_1$；等等。

证：i）上式左、右两边可看成关于X的首项系数为1的多项式。

ii）由于原根的个数是$\Phi(p^n-1)$，故左边的次数为$\Phi(p^n-1)$；再由逐步淘汰法则可知，右边的次数也为$\Phi(p^n-1)$。

iii）当$X\equiv f_\nu(x)$时，左边$\equiv 0$；而由$(f_\nu(x))^{p^n-1}\equiv 1$又可知右边$\equiv 0\ (\text{modd}\,p,\ \varphi(x))$。

由i）、ii）、iii）可知，该式子成立。

§10　原根

习题　证明所有的非零的互不同余的多项式之乘积$\equiv -1$ $(\text{modd}\,p,\ \varphi(x))$。

证：设　$f_1(x),\ f_2(x),\ \cdots,\ f_{p^n-1}(x)$

为重模p，$\varphi(x)$的一缩系，显然此缩系给出所有的非零的互不同余的多项式$(\text{modd}\,p,\ \varphi(x))$，并且是重模方程

$$X^{p^n-1}-1\equiv 0\ (\text{modd}\,p,\ \varphi(x))$$

的全部解，故有

$$X^{p^n-1}-1$$
$$\equiv (X-f_1(x))\cdots(X-f_{p^n-1}(x))(\text{modd}\,p,\varphi(x))$$

取$X\equiv 0$，就得到

$$-1\equiv(-1)^{p^n-1}f_1(x)\cdots f_{p^n-1}(x)(\text{modd}\,p,\ \varphi(x))$$

又因为$2\mid p^n-1$，故

$$-1\equiv f_1(x)\cdots f_{p^n-1}(x)(\text{modd}\,p,\ \varphi(x))$$

这就证明了本习题的结论。

第五章　素数分布之概况

一、提　　要

定义　设n过正整数趋向无穷(或x为一连续变数趋向无穷)。设$\varphi(n)$(或$\varphi(x)$)为n(或x)的正值函数，$f(n)$(或$f(x)$)为任一函数。若有一与n(或x)无关的数A，使$|f|\leqslant A\varphi$，则记为$f\ll\varphi$或者$f=O(\varphi)$。

定义　若$\lim\limits_{n\to\infty}\dfrac{f(n)}{\varphi(n)}=0$，则记为$f=o(\varphi)$。

定义　若$\lim\limits_{n\to\infty}\dfrac{f(n)}{\varphi(n)}=1$，则记为$f\sim\varphi$。

定理 1　$\sum\limits_{n=1}^{x}\dfrac{1}{n}=\log x+\gamma+O(\dfrac{1}{x})$，其中$\gamma$是Euler 常数。

定理 2　命

$$\operatorname{li}x=\lim_{\eta\to0}\left(\int_0^{1-\eta}+\int_{1+\eta}^{x}\right)\frac{dt}{\log t}$$

则

$$\operatorname{li}x\sim\frac{x}{\log x}.$$

定理 3　(Чебышев)命$\pi(x)$表不大于x的素数的个数，则

$$\frac{x}{\log x}\ll\pi(x)\ll\frac{x}{\log x}.$$

定理 4　素数的个数无限，即$\pi(x)$与x同趋向无穷。

定理 5 (Euler) 假定$f(n)$为一函数，对所有的正整数n，$f(n)$的值确定且不恒等于 0，并且 $(n, n')=1$ 时，$f(nn')=f(n)f(n')$，则

$$\sum_{n=1}^{\infty} f(n)=\prod_{p}(1+f(p)+f(p^2)+\cdots).$$

此等式成立的条件为：

(i)假定 $\sum_{n=1}^{\infty}|f(n)|$ 收敛，

或

(ii)假定 $\prod_{p}(1+|f(p)|+|f(p^2)|+\cdots)$ 收敛。

如果满足$f(nn')=f(n)f(n')$，则

$$\sum_{n=1}^{\infty} f(n)=\prod_{p}\frac{1}{1-f(p)}.$$

定理 6 级数 $\sum_{p}\frac{1}{p}$ 发散，p过所有素数。

定理 7 $\prod_{p}\left(1-\frac{1}{p}\right)$ 发散于零，p过所有素数。

定理 8

$$\lim_{n\to\infty}\frac{\pi(n)}{n}=0.$$

定理 9 当$n\geqslant 2$时，

$$\frac{1}{8}\leqslant\frac{\pi(n)}{\frac{n}{\log n}}\leqslant 12.$$

定理10 对任一实数$x\geqslant 1$，在x及$2x$之间必有一素数。

定理11 若$x\geqslant a$时，$f(x)$是一递增非负函数，则当$\xi\geqslant a$时有

$$\left|\sum_{a\leqslant n\leqslant \xi} f(n)-\int_{a}^{\xi} f(x)\,dx\right|\leqslant f(\xi).$$

定理12 设$x\geqslant a$时，$f(x)$是一递减非负函数，则极限

$$\lim_{n\to\infty}\left(\sum_{n=a}^{N}f(n)-\int_a^N f(x)\,dx\right)=\alpha$$

存在，且$0\leqslant\alpha\leqslant f(a)$。若$x\to\infty$时$f(x)\to 0$，则

$$\left|\sum_{a\leqslant n\leqslant\xi}f(n)-\int_a^{\xi}f(x)dx-\alpha\right|\leqslant f(\xi-1),(\xi\geqslant a+1)$$

定理13 当$\xi\geqslant 1$时，存在常数C，使

$$\left|\sum_{p\leqslant\xi}\frac{\log p}{p}-\log\xi\right|<C.$$

定理14 当$\xi\geqslant 2$时，存在常数C，使

$$\sum_{p\leqslant\xi}\frac{1}{p}=\log\log\xi+C+O\left(\frac{1}{\log\xi}\right).$$

定理15 当$\xi\geqslant 2$时，存在常数C，使

$$\prod_{p\leqslant\xi}\left(1-\frac{1}{p}\right)=\frac{C}{\log\xi}+O\left(\frac{1}{\log^2\xi}\right).$$

定义 命n为一正整数，$\omega(n)$表n的不同素因子的个数，$\Omega(n)$表n的全部素因子个数，即若

$$n=p_1^{a_1}\cdots p_s^{a_s}$$

则 $$\omega(n)=S,\ \Omega(n)=a_1+\cdots+a_s.$$

定理16

$$\sum_{n\leqslant x}\omega(n)=x\log\log x+c_1x+o(x)$$

$$\sum_{n\leqslant x}\Omega(n)=x\log\log x+c_2x+o(x).$$

其中c_1、c_2为正常数。

定理17

$$\omega(n)\sim\log\log n,$$

$$\Omega(n) \sim \log\log n.$$

定理18 有一实数α存在，如命

$$\alpha=\alpha_0,\quad 2^{\alpha_0}=\alpha_1,\quad \cdots,\quad 2^{\alpha_n}=\alpha_{n+1},\quad \cdots$$

则〔α_n〕常为一素数。

定理19 命$k>1$，形如$kn+1$的素数有无限多个。

定理20 若n为k的真因子，则对非± 1的整数x恒有

$$\left(x^n-1,\ \frac{x^k-1}{x^n-1}\right)\Big|\, k.$$

二、题 解

§4 素数之个数无限

习题1 证明形如$6n-1$之素数无限。

证：若形如$6n-1$的素数只有有限多个，设为p_1，p_2，…，p_m。

令 $N=6p_1p_2\cdots p_m-1$。显然N是形如$6n-1$的整数；如果N是素数，就与形如$6n-1$的素数只有p_1，…，p_m相矛盾。如果N是复合数，则一定有形如$6n-1$的素因子存在，因若N的素因子全为形如$6n+1$的数，则N必是形如$6n+1$的数。设此形如$6n-1$的素因子为p，由假定p是p_1，…，p_m中的一个，但$p_i\nmid N$（$1\leqslant i\leqslant m$），与$p|N$矛盾。这就证明了形如$6n-1$的素数无限。

习题2 证明形如$4n-1$之素数无限。

证：设p_1，…，p_m为形如$4n-1$的素数。

令 $$N=4p_1\cdots p_m-1$$

显然，N定有形如$4n-1$的素因子p，若不然，就和$N\equiv-1$

(mod 4) 矛盾。而p不与p_1，…，p_m中任何一个相同，故形如$4n-1$的素数无限。

习题 3 $\frac{\pi^2}{6}=\prod_p \frac{p^2}{p^2-1}$

证：设$f(n)=\frac{1}{n^2}$，显然$\sum_{n=1}^{\infty}|f(n)|$收敛且对任意正整数$n,n'$，都有$f(nn')=f(n)f(n')$，故由提要中定理5 Euler恒等式

$$\sum_{n=1}^{\infty} f(n)=\prod_p \frac{1}{1-f(p)}$$

得
$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\prod_p \frac{1}{1-\frac{1}{p^2}}=\prod_p \frac{p^2}{p^2-1}$$

又因为
$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6},$$

故
$$\frac{\pi^2}{6}=\prod_p \frac{p^2}{p^2-1}.$$

§7 Bertrand假设

习题 试用微积分方法计算

$$2^{\frac{2}{3}n}<(2n)^{\sqrt{2n}+1}$$

成立之界限。

解：把(1)式左右连取两次自然对数得

$$\ln 2+\ln n+\ln\ln 2<\ln 3+\ln(\sqrt{2n}+1)+\ln\ln 2n, \qquad (2)$$

显然，(1)、(2)成立的界限是相同的.下面就来计算(2)成立的界限。

设 $f(x)=\ln 3+\ln(\sqrt{2x}+1)+\ln\ln 2x-\ln 2-\ln x-\ln\ln 2$

则 $f'(x)=\frac{1}{2x+\sqrt{2x}}+\frac{1}{x\ln 2x}-\frac{1}{x}$

当$x\geqslant 4$时，$\ln 2x>2$，从而

$$\frac{1}{2x+\sqrt{2x}}+\frac{1}{x\ln 2x}<\frac{1}{2x}+\frac{1}{2x}=\frac{1}{x},$$

故$f'(x)<0$。此即当$x\geqslant 4$时，函数$f(x)$单调减少。又因为

$$f(467)>0,\ f(468)<0$$

且 $f(1)>0$，$f(2)>0$，$f(3)>0$

所以(2)成立的界限，亦即(1)成立的界限是

$$1\leqslant n\leqslant 467.$$

§8 以积分来估计和之数值

习题1 设ξ是整数，在

$$\sum_{1\leqslant n\leqslant \xi} n^{\lambda}=\frac{\xi^{\lambda+1}}{\lambda+1}+O(\xi^{\lambda})$$

中多求一项，即当$\lambda\geqslant 1$时，定出C使

$$\sum_{1\leqslant n\leqslant \xi} n^{\lambda}=\frac{\xi^{\lambda+1}}{\lambda+1}+C\xi^{\lambda}+O\left(\xi^{\lambda-1}\right)$$

解： 设

$$\varphi(\xi)=\sum_{1\leqslant a\leqslant \xi} n^{\lambda}-\frac{\xi^{\lambda+1}}{\lambda+1}$$

$$=\left(\xi-(\xi-1)\right)^{\lambda}+\left(\xi-(\xi-2)\right)^{\lambda}+\cdots+$$

$$+\xi^{\lambda}-\frac{\xi^{\lambda+1}}{\lambda+1}. \tag{1}$$

从

$$\sum_{1\leqslant n\leqslant\xi} n^{\lambda} = \frac{\xi^{\lambda+1}}{\lambda+1} + O(\xi^{\lambda})$$

知道存在正数A，使得

$$|\varphi(\xi)|\leqslant A\xi^{\lambda},$$

$$-A\xi^{\lambda}\leqslant\varphi(\xi)\leqslant A\xi^{\lambda}, \qquad (2)$$

此即$\varphi(\xi)$与ξ^{λ} 同阶，且(1)可写成

$$\varphi(\xi) = C\xi^{\lambda} + \varphi_1(\xi), \qquad (1')$$

其中C为非零常数，$\varphi_1(\xi)$至多与$\xi^{\lambda-1}$同阶．显然C满足$-A\leqslant C\leqslant A$，因若$C<-A$或$C>A$，那么当ξ充分大时就有

$$\varphi(\xi)<-A\xi^{\lambda},$$

或

$$\varphi(\xi)>A\xi^{\lambda},$$

但这两个不等式都与(2)相矛盾．从(1′)立得

$$\sum_{1\leqslant n\leqslant\xi} n^{\lambda} = \frac{\xi^{\lambda+1}}{\lambda+1} + C\xi^{\lambda} + O\left(\xi^{\lambda-1}\right)$$

其中C在$-A$和A之间．下面再用"面积原理"定出C在$\frac{1}{2}$和1之间，即证明

$$\frac{1}{2}\leqslant C<1.$$

为证此点，只需证明

$$\frac{1}{2}\xi^{\lambda}\leqslant\varphi(\xi)<1 \qquad (2')$$

即可．函数$f(x)=x^{\lambda}$，当$\lambda\geqslant1$时是下凸函数，如图所示：若用S表示面积，则从上图可以看出

$$\sum_{2\leqslant n\leqslant\xi} n^{\lambda} = S_{\square ABCD} + S_{\square EFGC} + \cdots + S_{\square HRST}$$

$$=\int_{1}^{\xi} x^{\lambda}\,dx + S_{\overparen{ABU}} + S_{\overparen{EFB}} + \cdots + S_{\overparen{HRV}} \tag{3}$$

并且 $S_{\overparen{ABU}} \geqslant S_{\Delta ABU} = \frac{1}{2}\left(2^{\lambda} - 1^{\lambda}\right)$

$$S_{\overparen{EFB}} \geqslant S_{\Delta EFB} = \frac{1}{2}\left(3^{\lambda} - 2^{\lambda}\right)$$

$$\cdots \quad \cdots \quad \cdots$$

$$S_{\overparen{HRV}} \geqslant S_{\Delta HRV} = \frac{1}{2}\left(\xi^{\lambda} - (\xi-1)^{\lambda}\right) \tag{4}$$

把(4)代入(3)得

$$\sum_{1\leqslant n\leqslant \xi} n^{\lambda} \geqslant \int_{1}^{\xi} x^{\lambda}\,dx + \frac{1}{2}\left(2^{\lambda} - 1^{\lambda}\right) + \frac{1}{2}\left(3^{\lambda} - 2^{\lambda}\right) + \cdots + \frac{1}{2}\left(\xi^{\lambda} - (\xi-1)^{\lambda}\right)$$

$$= \frac{\xi^{\lambda+1} - 1}{\lambda+1} + \frac{\xi^{\lambda} - 1}{2}$$

从而 $\sum_{1\leqslant n\leqslant \xi} n^{\lambda} \geqslant \frac{\xi^{\lambda+1} - 1}{\lambda+1} + \frac{\xi^{\lambda} - 1}{2} + 1$

$$= \frac{\xi^{\lambda+1}}{\lambda+1} + \frac{\xi^{\lambda}}{2} + \frac{1}{2} - \frac{1}{\lambda+1}$$

$$\geqslant \frac{\xi^{\lambda+1}}{\lambda+1} + \frac{\xi^{\lambda}}{2}$$

此即 $\varphi(\xi) \geqslant \frac{\xi^{\lambda}}{2}$ (5)

另一方面，从上图还可得到

$$\sum_{1\leqslant n\leqslant \xi} n^{\lambda} = S_{\square UB_1CD} + S_{\square BF_1GC} + \cdots + S_{\square VR_1ST} + S_{\square R_{ij}S}$$

$$< \int_1^{\xi} x^{\lambda} dx + S_{\square\mathrm{Rij8}}$$

$$= \frac{\xi^{\lambda+1} - 1}{\lambda + 1} + \xi^{\lambda}$$

此即 $$\varphi(\xi) < \xi^{\lambda} \qquad (6)$$

由(5)和(6)即得(2′)。这样就证明了

$$\sum_{1 \leqslant n \leqslant \xi} n^{\lambda} = \frac{\xi^{\lambda+1}}{\lambda+1} + C\xi^{\lambda} + O\left(\xi^{\lambda-1}\right)$$

其中常数C合条件$\frac{1}{2} \leqslant C < 1$.

习题2　引用定理1以研究和

$$\sum_{3 \leqslant n \leqslant \xi} \log\log n.$$

解：下面将证明

$$\sum_{3 \leqslant n \leqslant \xi} \log\log n = \xi \log\log\xi - \mathrm{li}\,\xi + C + O(\log\log\xi)$$

其中 $$\mathrm{li}\,\xi = \lim_{\eta \to 0} \left(\int_0^{1-\eta} + \int_{1+\eta}^{\xi} \right) \frac{dx}{\log x}$$

$$C = \lim_{\eta \to 0} \left(\int_0^{1-\eta} + \int_{1+\eta}^{3} \right) \frac{dx}{\log x} - 3\log\log 3$$

设 $$f(x) = \log\log x$$

显然$x \geqslant 3$时，它非负单调增加。由定理1（即提要中定理11）有

$$\left| \sum_{a \leqslant n \leqslant \xi} f(n) - \int_a^{\xi} f(x)\,dx \right| \leqslant f(\xi) \qquad (1)$$

因为 $$\sum_{1 \leqslant n \leqslant \xi} f(n) = \sum_{3 \leqslant n \leqslant \xi} \log\log n$$

$$\int_a^{\xi} f(x)\,dx = \int_3^{\xi} \log\log x\,dx =$$

$$=x\log\log x\Big|_3^{\xi}-\int_3^{\xi}\frac{dx}{\log x}$$

$$=\xi\log\log\xi-3\log\log 3-\mathrm{li}\,\xi+\lim_{\eta\to 0}\left(\int_0^{1-\eta}+\int_{1+\eta}^{3}\right)\frac{dx}{\log x}$$

且 $$f(\xi)=\log\log\xi$$

故把上面诸等式代入（1）即得所证。

习题3 证明当$\xi\geqslant 2$时

$$\sum_{1\leqslant n\leqslant\xi}\frac{\log n}{n}=\frac{1}{2}\log^2\xi+C_1+O\left(\frac{\log\xi}{\xi}\right).$$

证：由于 $$\sum_{1\leqslant n\leqslant\xi}\frac{\log n}{n}=\sum_{2\leqslant n\leqslant\xi}\frac{\log n}{n}$$

故只需证明 $$\sum_{1\leqslant n\leqslant\xi}\frac{\log n}{n}=\frac{1}{2}\log^2\xi+C_1+O\left(\frac{\log\xi}{\xi}\right)$$

即可。设 $$f(x)=\frac{\log x}{x}$$

当$x\geqslant 2$时$f(x)$非负递减且$\lim\limits_{x\to\infty}f(x)=0$。由提要中定理12可得

$$\left|\sum_{a\leqslant n\leqslant\xi}f(n)-\int_a^{\xi}f(x)\,dx-\alpha\right|\leqslant f(\xi-1)\qquad(1)$$

其中 $0\leqslant\alpha\leqslant f(2)$，$f(2)=\dfrac{\log 2}{2}$，$f(\xi-1)=\dfrac{\log(\xi-1)}{\xi-1}$

因为

$$\sum_{a\leqslant n\leqslant\xi}f(n)=\sum_{2\leqslant n\leqslant\xi}\frac{\log n}{n}$$

$$\int_a^{\xi}f(x)\,dx=\int_2^{\xi}\frac{\log x}{x}dx=\int_2^{\xi}\log x\,d\log x$$

$$=\frac{1}{2}\log^2 x\Big|_2^{\xi}=\frac{1}{2}\log^2\xi-\frac{1}{2}\log^2 2$$

且 $$\lim_{\xi\to\infty}\frac{\log(\xi-1)}{\xi-1}\Big/\frac{\log\xi}{\xi}=1$$

即任给$\varepsilon>0$，当ξ充分大时有

$$\frac{\log(\xi-1)}{\xi-1}\leqslant(1+\xi)\frac{\log\xi}{\xi}$$

把以上诸式代入（1）可得

$$\left|\sum_{2\leqslant n\leqslant\xi}\frac{\log n}{n}-\frac{1}{2}\log^2\xi+\frac{1}{2}\log^2 2-a\right|\leqslant(1+\varepsilon)\frac{\log\xi}{\xi}$$

此即 $$\sum_{2\leqslant n\leqslant\xi}\frac{\log n}{n}=\frac{1}{2}\log^2\xi+C_1+O\left(\frac{\log\xi}{\xi}\right)$$

其中 $$C_1=a-\frac{1}{2}\log^2 2.$$

习题4 证明当$\xi\geqslant2$时

$$\sum_{2\leqslant n\leqslant\xi}\frac{1}{n\log n}=\log\log\xi+C_2+O\left(\frac{1}{\xi\log\xi}\right).$$

证： 设$f(x)=\dfrac{1}{x\log x}$.

$x\geqslant2$时，$f(x)$非负递减且$\lim\limits_{x\to\infty}f(x)=0$。由定理12得

$$\left|\sum_{a\leqslant n\leqslant\xi}f(n)-\int_a^{\xi}f(x)\,dx-a\right|\leqslant f(\xi-1)\qquad(1)$$

其中 $0\leqslant a\leqslant f(2)$，$f(2)=\dfrac{1}{2\log2}$，$f(\xi-1)=\dfrac{1}{(\xi-1)\log(\xi-1)}$

因为 $$\sum_{a\leqslant n\leqslant\xi}f(n)=\sum_{2\leqslant n\leqslant\xi}\frac{1}{n\log n}$$

$$\int_a^{\xi} f(x)\,dx = \int_2^{\xi}\frac{1}{x\log x}\,dx = \int_2^{\xi}\frac{1}{\log x}d\log x$$

$$= \log\log x\Big|_2^{\xi} = \log\log\xi - \log\log 2$$

且 $$\lim_{\xi\to\infty}\frac{1}{(\xi-1)\log(\xi-1)}\Big/\frac{1}{\xi\log\xi} = 1$$

即任给$\varepsilon>0$，当ξ充分大时有

$$\frac{1}{(\xi-1)\log(\xi-1)}\leqslant(1+\varepsilon)\frac{1}{\xi\log\xi}$$

把以上诸式代入（1）可得

$$\left|\sum_{2\leqslant n\leqslant\xi}\frac{1}{n\log n}-\log\log\xi+\log\log 2-\alpha\right|\leqslant(1+\varepsilon)\frac{1}{\xi\log\xi}$$

$$\sum_{2\leqslant n\leqslant\xi}\frac{1}{n\log n}=\log\log\xi+C_2+O\left(\frac{1}{\xi\log\xi}\right),$$

其中 $C_2=\alpha-\log\log 2$。

§9 чебышев定理之推论

习题1 设p_n表示第n个素数，则存在正常数C_1、C_2，使

$$C_1 n\log n<p_n<C_2 n\log n.$$

证： 当$n\geqslant2$时，由提要中定理9得

$$\frac{1}{8}\cdot\frac{n}{\log n}\leqslant\pi(n)\leqslant12\cdot\frac{n}{\log n}$$

换n为p_n，有

$$\frac{1}{8}\cdot\frac{p_n}{\log p_n}\leqslant n\leqslant12\cdot\frac{p_n}{\log p_n}\tag{1}$$

不等式（1）左边给出

$$p_n\leqslant 8n\log p_n\tag{2}$$

两边取对数得

$$\log p_n \leqslant \log 8n + \log\log p_n \qquad (3)$$

又当$x>1$时，$\log x<\frac{x}{2}$，$\log\log p_n < \frac{1}{2}\log p$，因此由（3）得

$$\frac{1}{2}\log p_n < \log 8n$$

$$\log p_n < 2\lg 8n \leqslant 8\log n$$

再由（2）有

$$p_n \leqslant 8n\log p_n < 64n\log n \qquad (4)$$

而不等式（1）右边给出

$$p_n \geqslant \frac{1}{12}n\log p_n > \frac{1}{12}n\log n \qquad (5)$$

（4）、（5）并起来即得

$$\frac{1}{12}n\log n < p_n < 64n\log n。$$

习题2　存在正常数C，使

$$\varphi(n) > C\frac{n}{\log\log n} \quad (n\geqslant 3)。$$

证：因为

$$\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right)$$

故
$$\frac{n}{\log\log n} = \frac{\varphi(n)}{\prod\limits_{p|n}\left(1-\frac{1}{p}\right)\log\log n} \leqslant \frac{\varphi(n)}{\prod\limits_{p\leqslant n}\left(1-\frac{1}{p}\right)\log\log n} \qquad (1)$$

由提要中定理15，存在常数C_1，使得

$$\prod_{p\leqslant n}\left(1-\frac{1}{p}\right) = \frac{C_1}{\log n} + O\left(\frac{1}{\log^2 n}\right)$$

$$\log\log n\prod_{p\leqslant n}\left(1-\frac{1}{p}\right) = \frac{C_1\log\log n}{\log n} + O\left(\frac{\log\log n}{\log^2 n}\right)$$

又当$n\geqslant 3$时

$$\frac{\log\log n}{\log n}<\frac{1}{2},\qquad \frac{\log\log n}{\log^2 n}<\frac{1}{2\log 3}$$

因此 $\log\log n\prod_{p\leqslant n}\left(1-\frac{1}{p}\right)=O(1)$

而 $\log\log n\prod_{p\leqslant n}\left(1-\frac{1}{p}\right)>0,\quad (n\geqslant 3)$

故可找到两个正常数C、C_2，使得

$$C<\log\log n\prod_{p\leqslant n}\left(1-\frac{1}{p}\right)<C_2 \tag{2}$$

把（2）代入（1）有

$$\varphi(n)>C\cdot\frac{n}{\log\log n}.$$

习题3 试证无穷级数

$$\sum_p\frac{1}{p(\log\log p)h}$$

当$h>1$时收敛，当$h\leqslant 1$时发散．此处$\sum_p$表示通过所有素数。

证：（一）先证级数

$$\sum_{n=[e^3]}^{\infty}\frac{1}{n\log n(\log\log)^h}$$

当$h>1$时收敛，当$h\leqslant 1$时发散。

i） 当$h\neq 1$时

$$\int_{e^3}^{+\infty}\frac{dx}{x\log x(\log\lg ox)^h}=\frac{1}{1-h}\left[\frac{1}{(\log\log x)^{h-1}}\right]_{e^3}^{+\infty}$$

$$=\begin{cases}\dfrac{1}{(h-1)\log 3}, & h>1\\ +\infty, & h<1\end{cases}$$

ii）当$h=1$时

$$\int_{e^3}^{+\infty}\frac{dx}{x\log x(\log\log x)^h}=\int_{e^3}^{+\infty}\frac{dx}{x\log x(\log\log x)}$$

$$=\int_{e^3}^{+\infty}\frac{d(\log\log x)}{\log\log x}=[\log\log\log x]_{e^3}^{+\infty}=+\infty$$

从而由积分判定法可知级数

$$\sum_{n=[e^3]}^{\infty}\frac{1}{n\log n(\log\log n)^h}$$

当$h>1$时收敛，当$h\leqslant1$时发散。

（二）再证级数

$$\sum_{n=1}^{\infty}\frac{1}{p_n(\log\log p_n)^h}$$

当$h>1$时收敛，当$h\leqslant1$时发散。

i）当$h>1$时

由习题1有$p_n>\frac{1}{12}n\log n$。又因$\log\log p_n>\log\log n$，故有

$$\frac{1}{p_n(\log\log p_n)^h}<\frac{12}{n\log n(\log\log n)^h},$$

由（一），级数$\sum_{n=1}^{\infty}\frac{1}{p_n(\log\log p_n)^h}$ 收敛

ii）当$0<h\leqslant1$时

由习题1有$\log p_n<8\log n$，$\log\log p_n<\log 8+\log\log n$

且$p_n<64n\log n$

故 $$\frac{1}{p_n(\log\log p_n)^h}>\frac{1}{64n\log n(\log\log n+\log 8)^h}$$

由于 $$\frac{1}{n\log n(\log\log n+\log 8)^h}\sim\frac{1}{n\log n(\log\log n)^h}$$

且（一）指出级数

$$\sum_{n=[e^3]}^{\infty}\frac{1}{n\log n(\log\log n)^h}$$

发散，故级数

$$\sum_{n=1}^{\infty}\frac{1}{p_n(\log\log p_n)^h}$$

发散。

iii）当$h\leqslant 0$时

由于
$$\frac{1}{p_n(\log\log p_n)^h}\geqslant\frac{1}{p_n}$$

故从级数

$$\sum_{n=1}^{\infty}\frac{1}{p_n}$$

的发散性，可知级数

$$\sum_{n=1}^{\infty}\frac{1}{p_n(\log\log p_n)^h}$$

发散。注意到

$$\sum_{p}\frac{1}{p(\log\log p)^h}=\sum_{n=1}^{\infty}\frac{1}{p_n(\log\log p_n)^h}$$

由（一）、（二）即得所证。

§11　表素数之函数

习题1　证明并无一个非常数的整系数多项式$f(x)$，能对任一整数n，$f(n)$常为素数。

证： 如若不然，可设

$$f(x)=a_0+a_1x+\cdots+a_mx^m,\quad a_m\neq 0$$

为一非常数的整系数多项式，且对任一的整数n，$f(n)$ 常为素数。此时显然有$a_0 \neq 0$，± 1，否则0、± 1都是素数。

i）当$a_0 = p$，p为素数时，由于

$$a_1x + a_2x^2 + \cdots + a_mx^m$$

最多只有m个整数根，故在序列

$$\{a_1p^s + \cdots + a_mp^{ms}\}, s = 1, 2, \cdots$$

中，必然有$s = K$，使得

$$a_1p^K + \cdots + a_mp^{mK} \neq 0$$

$$f(p^K) = p + a_1p^K + \cdots + a_mp^{mK}$$
$$= p(1 + a_1p^{K-1} + \cdots + a_mp^{mK-1})$$

故有　$p|f(p^K)$，且$f(p^K) \neq p$，

此与$f(n)$常为素数矛盾。

ii）当$a_0 = p_1 \cdots p_t$，$t \geqslant 2$及p_1，$\cdots$，p_t为素数时，取$n = a_0$，就有

$$f(n) = f(a_0) = a_0 + a_1a_0 + \cdots + a_m a_0{}^m$$
$$= a_0(1 + a_1 + \cdots + a_m a_0{}^{m-1})$$

从而$p_i|f(n)$，$(1 \leqslant i \leqslant t)$，此也与$f(n)$常为素数矛盾。由i）、ii）可知，并无一个非常数的整系数多项式$f(x)$，能对任一整数n，$f(n)$常为素数。

习题7　命$P(x_1, x_2, \cdots, x_k)$表一整系数多项式。命

$$f(n) = P(n, 2^n, \cdots, k^n).$$

若当$n \to \infty$时，$f(n) \to \infty$，则$f(n)$代表无穷个复合数。

证：设

$$P(x_1, x_2, \cdots, x_k) = \sum_{i=0}^{m} P_i(x_1, x_2, \cdots, x_k)$$

其中P_i表i次齐次多项式。下面对m行归纳法以证明本题的结论。

当$m = 1$时

$$P(x_1, x_2, \cdots, x_k) = P_0 + P_1(x_1, x_2, \cdots, x_k)$$

设　$P_1(x_1, x_2, \cdots, x_k) = a_1x_1 + a_2x_2 + \cdots + a_kx_k$

则 $P(n, 2^n, \cdots, k^n) = P_0 + a_1 n + a_2 2^n + \cdots + a_k k^n$. 并且因为 $n \to \infty$ 时 $f(n) \to \infty$，故 $f(n)$ 可表无穷多个整数且存在正整数 N，当 $n \geqslant N$ 时，$f(n)$ 是递增的，即

$$f(N) < f(N+1) < f(N+2) < \cdots < \cdots \qquad (1)$$

如果 $n = N$ 时，$f(N) = q$，q 为素数．不失一般，可设

$$(a_1, q) = (k!, q) = 1$$

于是存在正整数 r 使得

$$a_1 r \equiv 1 \pmod{q}$$

设 $$q_r = f\left(r(q-1)(P_0 + a_2 + \cdots + a_k)\right)$$

那么序列

$$\{q_{r+sq}\}, \quad s = 0, 1, 2, \cdots$$

中至少有一个复合数．如若不然，由

$$q_r = P_0 + a_1 r(q-1)(P_0 + a_2 + \cdots + a_k) +$$
$$+ a_2 2^{r(q-1)(P_0 + a_2 + \cdots + a_k)} + \cdots + a_k k^{r(q-1)(P_0 + a_2 + \cdots + a_k)}$$
$$\equiv P_0 - (P_0 + a_2 + \cdots + a_k) + a_2 + \cdots + a_k$$
$$\equiv 0 \pmod{q},$$

可得 $$q_{r+sq} \equiv 0 \pmod{q}$$

再因为 q_{r+sp} 为素数，就得 $q_{r+sq} = q$，与(1)相矛盾．这证明，对于充分大的 N，如果 $f(N)$ 为素数，则一定有 $n > N$ 使得 $f(n)$ 为复合数．由于 $f(n)$ 可表无穷多个整数，因此也就可表无穷多个复合数．故当 $m = 1$ 时

$$P(n, 2^n, \cdots, k^n)$$

可表无穷多个复合数．归纳假定 $m \leqslant t$ 时结论成立．那么，当 $m = t + 1$ 时，由于

$$P'_{x_1}(x_1, x_2 \cdots, x_k)$$

的次数 $\leqslant t$，因而归纳假定保证

$$P'_{x_1}(n, 2^n, \cdots, k^n)$$

可表无穷多个复合数．设R是任一可经

$$P'_{x_1}(n, 2^n, \cdots, k^n)$$

表出的一个复合数，即存在正整数n，使

$$P'_{x_1}(n, 2^n, \cdots, k^n)-R=0.$$

命 $$F=P(x_1, x_2, \cdots, x_k)-Rx_1$$

由 $$F'_{x_1}=P'_{x_1}(x_1, x_2, \cdots, x_k)-R=0$$

有解$(n, 2^n, \cdots, k^n)$，可知

$$F=P(x_1, x_2, \cdots x_k)-Rx_1$$

有解$(n, 2^n,\cdots,k^n)$，此即对任一确定的R，可找到n，使

$$P(n, 2^n, \cdots, k^n)=Rn,$$

再由归纳假定知道R有无穷多个，故当$m=t+1$时，

$$P(n,2^n, \cdots,k^n)$$

可表无穷多个复合数．

§12 等差级数中之素数问题

习题 有无穷个形如$8n+5$之素数．

证：如果形如$8n+5$的素数不是无穷个而是有限个，设为

$$p_1, p_2, \cdots, p_s$$

取 $$N=(p_1p_2\cdots p_s)^2+4$$

则 $$N\equiv 5(\bmod 8)$$

设q为N的任一素因子，那么由

$$(p_1p_2\cdots p_s)^2\equiv -4(\bmod q)$$

$$\left(\frac{-4}{q}\right)=\left(\frac{-1}{q}\right)=(-1)^{\frac{1}{2}(q-1)}=1$$

知道$q\equiv 1(\bmod 4)$，从而可知

N的任一素因子$\equiv 1$或$5(\bmod 8)$

下面证明N至少有一素因子$p\equiv 5(\bmod 8)$，否则，由N的素因子

都$\equiv 1 \pmod 8$，就有

$$N \equiv 1 \pmod 8$$

这与

$$N \equiv 5 \pmod 8$$

相矛盾，而p与p_1，…，p中任何一个都不相同，这又与形如$8n+5$的素数只有p_1，…，p相矛盾．故形如$8n+5$的素数有无穷多个．

第六章　数论函数

一、提　要

定义　对任一正整数n，都有一定数值的函数$f(n)$称为数论函数。

定义　若数论函数$f(n)$对于$(a,b)=1$，有$f(ab)=f(a)f(b)$，则称$f(n)$为积性函数；若不论有无$(a,b)=1$，都有$f(ab)=f(a)f(b)$，则称$f(n)$为完全积性函数。

例1　函数

$$\Delta(n)=\begin{cases}1, & 若n=1\\ 0, & 若n\neq 1\end{cases}$$

是一完全积性函数。

例2　函数

$$E_\lambda(n)=n^\lambda$$

是一完全积性函数。

例3　Möbius函数

$$\mu(n)=\begin{cases}1, & 若n=1\\ (-1)^r, & 若n为r个不同素数的积\\ 0, & 若n为一素数的平方所整除\end{cases}$$

是一积性函数，但不是完全积性函数。

例4　Euler函数$\varphi(n)$是一积性函数，但不是完全积性函数。

例5　除数函数

$$d(n)=\sum_{d|n}1$$

是积性函数，但不是完全积性函数．一般的，

$$\sigma_\lambda(n)=\sum_{d|n}d^\lambda$$

也是一积性函数．显然$\sigma_0(n)=d(n)$．

例6 Von Mangoldt函数

$$\Lambda(n)=\begin{cases}\log p, & \text{若}n\text{为素数}p\text{的正乘方}\\ 0, & \text{不然}\end{cases}$$

是一非积性函数．

例7 命$r(n)$表$n=x^2+y^2$的解数，那么$\frac{1}{4}r(n)$是积性函数，但不是完全积性函数．

定理1 若$f(n)$是一非恒等于零的积性函数，则

$$\sum_{d|n}\mu(d)f(d)=\prod_{p|n}\left(1-f(p)\right)$$

此处p过n的不同的素因子．

定理2 命$h(k)$表一非恒等于零的完全积性函数，又n_0是一正整数．若对所有$n\leqslant n_0$，常有

$$g(n)=\sum_{d|n}f(d)h\left(\frac{n}{d}\right)$$

则对此n也有

$$f(n)=\sum_{d|n}\mu(d)g\left(\frac{n}{d}\right)h(d)$$

反过来也是成立的．

定义 若 $$g(n)=\sum_{d|n}f(d)=\sum_{d|n}f\left(\frac{n}{d}\right)$$

则$g(n)$称为$f(n)$的Möbius变换，而$f(n)$称为$g(n)$的Möbius逆变换。

定理3　$\varphi(n)=n\sum_{d|n}\frac{\mu(d)}{d}$ 。

定理4　$d(mn)\leqslant d(m)d(n)$。

定理5　对任一$\varepsilon>0$，都有

$$d(n)=O(n^{\varepsilon})。$$

O中常数只与ε有关。

定理6　若$\xi\geqslant 1$，则

$$\sum_{1\leqslant n\leqslant\xi}d(n)=\xi\log\xi+(2\gamma-1)\xi+O(\sqrt{\xi})$$

此处γ是Euler常数。

定义　若有一正整数组，其中不大于x的个数$N(x)$适合

$$\lim_{x\to\infty}\frac{N(x)}{x}=a$$

则此组数出现的概率记为a。

定义　一正整数若不能被素数平方整除，则称它为无平方因子。

定理7　不超过x的无平方因子数的个数为

$$\frac{6}{\pi^2}x+O(\sqrt{x})$$

由此可知无平方因子数出现的概率为$\frac{6}{\pi^2}$。

定义

$$\chi(n)=\begin{cases}0, & 若2|n\\ (-1)^{\frac{1}{2}(n-1)}, & 若2\nmid n\end{cases}$$

$$\delta(n)=\sum_{d|n}\chi(d)$$

定理8 同余式

$$x^2 \equiv -1 \pmod{n}$$

的解数$V(n)$等于

$$V(n)=\begin{cases} 0, & 若4|n \\ \prod_{p|n}\left(1+\chi(p)\right), & 若4\nmid n \end{cases}$$

定理9 命$r(n)$表方程

$$x^2+y^2=n$$

的整数解x、y的组数，则

$$r(n)=4\delta(n),$$

定理10 命$n>1$，对应于

$$l^2\equiv -1 \pmod{n}$$

的一个解，有一对且唯有一对整数x、y，使

$$x^2+y^2=n,\quad x>0,\quad y>0$$

$$(x,\ y)=1,\quad y\equiv lx \pmod{n}.$$

定理11 把一整数n分为两个平方和的方法数的四分之一，等于n的因子$\equiv 1 \pmod{4}$的个数减去n的因子$\equiv 3 \pmod{4}$的个数。

定理12 对任一ε，常有

$$r(n)=O(n^{\varepsilon}).$$

定理13 $$\sum_{1\leqslant r\leqslant x} r(n)=\pi x+O(\sqrt{x}).$$

定理14 命l表示一有长的简单闭曲线的长度，而以A表示曲线所围区域的面积，N为曲线内所含整点的个数，则若$l\geqslant 1$，必有

$$|A-N|<l.$$

定义 n级Farey贯，是指0和1之间，其分母$\leqslant n$，且依大小次序排列的既约分数。即依大小排列的形如

$\frac{a}{b}$，$(a, b)=1$，$0 \leqslant a \leqslant b \leqslant n$的诸分数。

定理15 设

$$\frac{a}{b}<\frac{a''}{b''}<\frac{a'}{b'}$$

为Farey贯中的三邻项，则

i) $\frac{a''}{b''}=\frac{a+a'}{b+b'}$;

ii) $ba''-b''a=b''a'-b'a''=1$;

iii) $b+b'' \geqslant n+1$，$b''+b' \geqslant n+1$.

定理16 命ξ为一实数，则在n级Farey贯中必有一数$\frac{a}{b}$，使

$$\left|\xi-\frac{a}{b}\right|<\frac{1}{bn},\quad 0<b \leqslant n.$$

定理17 任给二实数ξ，$\eta \geqslant 1$，必有有理数$\frac{a}{b}$，使

$$\left|\xi-\frac{a}{b}\right|<\frac{1}{b\eta},\quad 0<b \leqslant \eta.$$

定理18 任给一实数ξ，必有有理数$\frac{a}{b}$，使

$$\left|\xi-\frac{a}{b}\right|<\frac{1}{b^2}$$

若ξ为无理数，则有无数个$\frac{a}{b}$适合此式。

定理19 任给一无理数ξ，必有无数个有理数$\frac{a}{b}$存在，使

$$\left|\xi-\frac{a}{b}\right|<\frac{1}{\sqrt{5}b^2}.$$

定理20 设m为整数，$A>2$，$1\leqslant m\leqslant A^{\frac{1}{3}}$，$(a, m)=1$，$k\geqslant 1$．又设

$$S=\sum_{x=M}^{M+m-1}\{f(x)\}$$

此处$f(x)$在$M\leqslant x\leqslant M+m-1$中定义，并有连续二阶导数，且满足于

$$f'(M)=\frac{a}{m}+\frac{\theta}{m^2},\quad (a, m)=1,\ |\theta|<1,$$

$$\frac{1}{A}\leqslant|f''(x)|\leqslant\frac{k}{A}\quad ,$$

则
$$\left|S-\frac{1}{2}m\right|\leqslant\frac{1}{2}(k+5).$$

定理21 用$R(x)$记圆

$$u^2+v^2\leqslant x$$

内的整点数，则当$x\geqslant 2$时，

$$R(x)=\pi x+O(x^{\frac{1}{3}}\log x).$$

定理22 若$\xi\geqslant 2$，则

$$\sum_{1\leqslant n\leqslant\xi}d(n)=\xi\log\xi+(2\gamma-1)\xi+O(\xi^{\frac{1}{3}}\log^2\xi).$$

定义 函数

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$$

称为Riemannζ函数．

定理23 当$s>1$时，

$$\zeta(s)=\prod_p\left(1-\frac{1}{p^s}\right)^{-1}.$$

二、题　解

§4 Möbius变换.

习题1　若$g(n)$及$g_1(n)$各为$f(n)$及$f_1(n)$之Möbius变换，试证明

$$\sum_{d|n} g(d) f_1\left(\frac{n}{d}\right) = \sum_{d|n} f(d) g_1\left(\frac{n}{d}\right).$$

证：

$$\sum_{d|n} g(d) f_1\left(\frac{n}{d}\right) = \sum_{d|n} f_1(d) g\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} f_1(d) \sum_{d_1 | \frac{n}{d}} f(d_1) = \sum_{d|n} \sum_{d_1 | \frac{n}{d}} f_1(d) f(d_1)$$

$$= \sum_{d_1|n} \sum_{d | \frac{n}{d_1}} f_1(d) f(d_1) = \sum_{d_1|n} f(d_1) \sum_{d | \frac{n}{d_1}} f_1(d)$$

$$= \sum_{d_1|n} f(d_1) g_1\left(\frac{n}{d_1}\right) = \sum_{d|n} f(d) g_1\left(\frac{n}{d}\right).$$

习题2　求出$g(n)g_1(n)$之Möbius逆变换.

解： 设$F(n)=g(n)g_1(n)$的Möbius逆变换为$\varphi(n)$,则由定义得

$$\varphi(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) g_1\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) g_1(d).$$

习题3　$f(n)$之Möbius变换之Möbius变换等于

$$\sum_{d_1\mid n} f(d_1)d\left(\frac{n}{d_1}\right)$$

证：设$f(n)$的Möbius变换为$g(n)$，$g(n)$的Möbius变换为$G(n)$，那么

$$G(n)=\sum_{d\mid n} g(d)=\sum_{d\mid n} g\left(\frac{n}{d}\right)$$

$$=\sum_{d\mid n}\sum_{d_1\mid\frac{n}{d}} f(d_1)=\sum_{d_1\mid n}\sum_{d\mid\frac{n}{d_1}} f(d_1)$$

$$=\sum_{d_1\mid n} f(d_1)\sum_{d\mid\frac{n}{d_1}} 1$$

$$=\sum_{d_1\mid n} f(d_1)d\left(\frac{n}{d_1}\right).$$

习题4　用证明例6之方法证明4.10(1)式。

证：此题系指用Möbius变换证明下式

$$\prod_{v}\left(X-f_v(x)\right)\equiv\frac{X^{p^n-1}-1}{\prod_{q}\left(X^{(p^n-1)/q}-1\right)}\cdot$$

$$\frac{\prod_{q,q_1}\left(X^{(p^n-1)/qq_1}-1\right)}{\prod_{q,q_1,q_2}\left(X^{(p^n-1)/qq_1q_2}-1\right)}\cdots\left(\bmod\, p,\ \varphi(x)\right)$$

此处$f_v(x)$过所有原根，$\prod_{q}$过p^n-1的所有素因子q，$\prod_{q,q_1}$过p^n-

1的所有素因子对q、q_1，且$q\neq q_1$，等等．设Φ_d表对重模p，$\varphi(x)$次数为d的多项式的个数，再设$N=p^n-1$．由于重模p，$\varphi(x)$的缩系所含多项式的个数为N，因此

$$\sum_{d|N}\Phi_d=N$$

此即N是Φ_N的Möbius变换．由反转公式有

$$\Phi_N=\sum_{d|N}\frac{N\mu(d)}{d}$$

此式表上式左右两端关于X的次数相等．另一方面，当

$X\equiv f_\nu(x)(\bmod d p,\ \varphi(x))$，$\nu=1,\ 2,\ \cdots,\ \Phi_N$

时，上式成立(左右两端$\equiv 0(\bmod d p,\ \varphi(x))$，且两端都是首项系数为1的多项式，故上式成立．

§5 除数函数

习题1 证明：当$\xi\geqslant 2$时，

$$\sum_{1\leqslant n\leqslant\xi}\frac{d(n)}{n}=\frac{1}{2}\log^2\xi+2\gamma\log\xi+C+O\left(\xi^{-\frac{1}{2}}\log\xi\right).$$

证：我们证明下面一个较习题结论精确的等式

$$\sum_{1\leqslant n\leqslant\xi}\frac{d(n)}{n}=\frac{1}{2}\log^2\xi+2\gamma\log\xi+C+O\left(\xi^{-1}\log\xi\right)$$

从而习题结论也就被证明了．此等式的证明要用到：

$$\sum_{1\leqslant n\leqslant\xi}\frac{1}{n}=\log\xi+\gamma+O\left(\frac{1}{\xi}\right)$$

$$\sum_{1\leqslant n\leqslant\xi}\frac{\log n}{n}=\frac{1}{2}\log^2\xi+C_1+O\left(\xi^{-1}\log\xi\right)$$

以上二式分别为第五章定理 1 和第五章第八节习题 3 的结论。

$$\sum_{1\leqslant n\leqslant\xi}\frac{d(n)}{n}=\sum_{1\leqslant n\leqslant\xi}\frac{1}{n}\sum_{u|n}1$$

如果令$n=uv$，就有

$$\sum_{1\leqslant n\leqslant\xi}\frac{d(n)}{n}=\sum_{1\leqslant u\leqslant\xi}\frac{1}{u}\sum_{1\leqslant v\leqslant\xi/u}\frac{1}{v}$$

$$=\sum_{1\leqslant u\leqslant\xi}\frac{1}{u}\left(\log\frac{\xi}{u}+\gamma+O\left(\frac{u}{\xi}\right)\right)$$

$$=\sum_{1\leqslant u\leqslant\xi}\frac{1}{u}\left(\log\xi-\log u\right)+\gamma\sum_{1\leqslant u\leqslant\xi}\frac{1}{u}+\sum_{1\leqslant u\leqslant\xi}O\left(\frac{1}{\xi}\right)$$

$$=(\log\xi+\gamma)\sum_{1\leqslant u\leqslant\xi}\frac{1}{u}-\left(\frac{1}{2}\log^2\xi+C_1+O(\xi^{-1}\log\xi)\right)+O(1)$$

$$=(\log\xi+\gamma)\left(\log\xi+\gamma+O\left(\frac{1}{\xi}\right)\right)-$$

$$-\left(\frac{1}{2}\log^2\xi+C_1+O(\xi^{-1}\log\xi)\right)+O(1)$$

$$=\log^2\xi+2\ \log\xi+O(\xi^{-1}\log\xi)+\gamma^2+O\left(\frac{\gamma}{\xi}\right)-$$

$$-\frac{1}{2}\log^2\xi-C_1-O(\xi^{-1}\log\xi)+O(1)$$

$$=\frac{1}{2}\log^2\xi+2\gamma\log\xi+C+O(\xi^{-1}\log\xi)$$

其中$C=\gamma^2-C_1+O(1)$。

习题2　证明：对任一ε，常有

$$\sigma(n)=O(n^{1+\varepsilon})。$$

证：命$n=\prod_{p|n}p^a$表n的标准分解式，则

$$\frac{\sigma(n)}{n^{1+\varepsilon}}=\prod_{p|n}\frac{p^{a+1}-1}{p-1}\cdot\frac{1}{p^{a(1+\varepsilon)}}$$

$$=\prod_{p|n}\frac{p^{a}+p^{a-1}+\cdots+p+1}{p^{a(1+\varepsilon)}}$$

$$=\prod_{p|n}\frac{1+\frac{1}{p}+\cdots+\frac{1}{p^{a}}}{p^{a\varepsilon}}\leqslant\prod_{p|n}\frac{a+1}{p^{a\varepsilon}} \qquad (1)$$

任一$\varepsilon>0$

$$p^{a\varepsilon}\geqslant 2^{a\varepsilon}=e^{a\varepsilon\log 2}\geqslant a\varepsilon\log 2\geqslant\frac{1}{2}(a+1)\varepsilon\log 2,$$ 且若$p^{\varepsilon}\geqslant 2$，则

$$p^{a\varepsilon}\geqslant 2^{a}\geqslant a+1$$

故有 $$\prod_{p|n}\frac{a+1}{p^{a\varepsilon}}=\prod_{\substack{p|n\\p^{\varepsilon}<2}}\frac{a+1}{p^{a\varepsilon}}\prod_{\substack{p|n\\p^{\varepsilon}>2}}\frac{a+1}{p^{a\varepsilon}}\leqslant\prod_{\substack{p|n\\p^{\varepsilon}<2}}\frac{a+1}{\frac{1}{2}(a+1)\varepsilon\log 2}\cdot$$

$$\prod_{\substack{p|n\\p^{\varepsilon}>2}}\frac{a+1}{a+1}\leqslant\prod_{p^{\varepsilon}<2}\frac{2}{\varepsilon\log 2}, \qquad (2)$$

把（2）代入（1），即得

$$\sigma(n)=O(n^{1+\varepsilon}).$$

习题3 证明：当$\xi\geqslant 2$时，

$$\sum_{1\leqslant n\leqslant\xi}\sigma(n)=\frac{1}{12}\pi^{2}\xi^{2}+O(\xi\log\xi).$$

证： 在证明中要用到

$$\sum_{n=1}^{\infty}\frac{1}{n^{2}}=\frac{\pi^{2}}{6},\quad\sum_{n\geqslant\xi}\frac{1}{n^{2}}=O\left(\frac{1}{\xi}\right).$$

$$\sum_{1\leqslant n\leqslant\xi}\sigma(n)=\sum_{1\leqslant n\leqslant\xi}\sum_{d|n}d=$$

$$= \sum_{dd_1 \le \xi} d_1 = \sum_{d=1}^{[\xi]} \sum_{d_1=1}^{[\xi/d]} d_1$$

$$= \sum_{d=1}^{[\xi]} \frac{1}{2}\left[\frac{\xi}{d}\right]\left(\left[\frac{\xi}{d}\right]+1\right)$$

$$= \frac{1}{2}\sum_{d=1}^{[\xi]}\left(\left[\frac{\xi}{d}\right]^2+\left[\frac{\xi}{d}\right]\right)$$

$$= \frac{1}{2}\sum_{d=1}^{[\xi]}\left(\frac{\xi^2}{d^2}+O\left(\frac{\xi}{d}\right)\right)$$

$$= \frac{1}{2}\xi^2\sum_{d=1}^{[\xi]}\frac{1}{d^2}+O\left(\xi\sum_{d=1}^{[\xi]}\frac{1}{d}\right)$$

$$= \frac{1}{2}\xi^2\sum_{d=1}^{\infty}\frac{1}{d^2}+O\left(\xi^2\sum_{d=[\xi]+1}^{\infty}\frac{1}{d^2}\right)+O(\xi\log\xi)$$

$$= \frac{1}{2}\xi^2\frac{\pi^2}{6}+O(\xi)+O(\xi\log\xi)$$

$$= \frac{1}{12}\pi^2\xi^2+O(\xi\log\xi).$$

§7 表整数为二平方之和

习题1 试证恒等式：

$$(x_1{}^2+x_2{}^2+x_3{}^2+x_4{}^2)(y_1{}^2+y_2{}^2+y_3{}^2+{}_4{}^2)$$
$$=x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+(x_1y_2-x_2y_1+x_3y_4-$$
$$-x_4y_3)^2+(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2+(x_1y_4-x_4y_1+$$
$$+x_2y_3-x_3y_2)^2.$$

证：因为

$$(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2=$$

$$=x_1^2y_1^2+x_2^2y_2^2+x_3^2y_3^2+x_4^2y_4^2+2x_1x_2y_1y_2+$$
$$+2x_1x_3y_1y_3+2x_1x_4y_1y_4+2x_2x_3y_2y_3+2x_2x_4y_2y_4+$$
$$+2x_3x_4y_3y_4,$$

$$(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2$$
$$=x_1^2y_2^2+x_2^2y_1^2+x_3^2y_4^2+x_4^2y_3^2-2x_1x_2y_1y_2+$$
$$+2x_1x_3y_2y_4-2x_1x_4y_2y_3-2x_2x_3y_1y_4+2x_2x_4y_1y_3-$$
$$-2x_3x_4y_3y_4,$$

$$(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2$$
$$=x_1^2y_3^2+x_3^2y_1^2+x_4^2y_2^2+x_2^2y_4^2-2x_1x_3y_1y_3+$$
$$+2x_1x_4y_2y_3-2x_1x_2y_3y_4-2x_3x_4y_1y_2+2x_2x_3y_1y_4-$$
$$-2x_2x_4y_2y_4,$$

$$(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2$$
$$=x_1^2y_4^2+x_4^2y_1^2+x_2^2y_3^2+x_3^2y_2^2-2x_1x_4y_1y_4+$$
$$+2x_1x_2y_3y_4-2x_1x_3y_2y_4-2x_2x_4y_1y_3+2x_3x_4y_1y_2-$$
$$-2x_2x_3y_2y_3,$$

故　右边$=x_1^2y_1^2+x_1^2y_2^2+x_1^2y_3^2+x_1^2y_4^2+x_2^2y_1^2+$
$$+x_2^2y_2^2+x_2^2y_3^2+x_2^2y_4^2+x_3^2y_1^2+x_3^2y_2^2+$$
$$+x_3^2y_3^2+x_3^2y_4^2+x_4^2y_1^2+x_4^2y_2^2+x_4^2y_3^2+$$
$$+x_4^2y_4^2$$
$$=(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)$$
$=$左边。

习题2　试证恒等式：

$$(x_1^2+x_2^2+x_3^2+x_4^2+x_5^2+x_6^2+x_7^2+x_8^2)\times$$
$$\times(y_1^2+y_2^2+y_3^2+y_4^2+y_5^2+y_6^2+y_7^2+y_8^2)$$
$$=(x_1y_1+x_2y_2+x_3y_3+x_4y_4+x_5y_5+x_6y_6+x_7y_7+x_8y_8)^2+$$
$$+(x_1y_2-x_2y_1-x_3y_4+x_4y_3-x_5y_6+x_6y_5-x_7y_8+x_8y_7)^2+$$
$$+(x_1y_3+x_2y_4-x_3y_1-x_4y_2+x_5y_7-x_6y_8-x_7y_5+x_8y_6)^2+$$
$$+(x_1y_4-x_2y_3+x_3y_2-x_4y_1-x_5y_8-x_6y_7+x_7y_6+x_8y_5)^2+$$

$$+(x_1y_5+x_2y_6-x_3y_7+x_4y_8-x_5y_1-x_6y_2+x_7y_3-x_8y_4)^2+$$
$$+(x_1y_6-x_2y_5+x_3y_8+x_4y_7+x_5y_2-x_6y_1-x_7y_4-x_8y_3)^2+$$
$$+(x_1y_7+x_2y_8+x_3y_5-x_4y_6-x_5y_3+x_6y_4-x_7y_1-x_8y_2)^2+$$
$$+(x_1y_8-x_2y_7-x_3y_6-x_4y_5+x_5y_4+x_6y_3+x_7y_2-x_8y_1)^2.$$

证： 证法同习题1，此处从略。

§9 圆内整点问题

习题1 求出以原点为中心之椭圆中整点个数之渐近公式。

解： 设以原点为中心，长短半轴各为x、y的椭圆面积为A，周长为L，椭圆内部整点数为N，那么

$$A=\pi xy$$

$$L=4x\cdot\frac{\pi}{2}\left[1-\left(\frac{1}{2}\right)^2e^2-\left(\frac{1\cdot3}{2\cdot4}\right)^2\frac{e^4}{3}-\right.$$
$$\left.-\left(\frac{1\cdot3\cdot5}{2\cdot4\cdot6}\right)^2\frac{e^6}{5}-\cdots\right]<2\pi x.$$

由提要中定理14 $\quad |A-N|<L$

有 $\quad |\pi xy-N|<2\pi x$

故 $\quad N=\pi xy+O(x).$

习题2 证明球

$$u^2+v^2+w^2\leqslant x$$

内整点数$=\frac{4}{3}\pi x^{\frac{3}{2}}+O(x)$.

证： 在空间中过整点分别作与三个坐标面平行的平面，这些平面把空间分为立方格子，一球内整点对应于一立方格，其八个顶点坐标为：

$$(u,\ v,\ w),\ (u,\ v+1,\ w),$$
$$(u-1,\ v+1,\ w),\ (u-1,\ v,\ w),$$

$$(u,\ v,\ w+1),\ (u,\ v+1,\ w+1),$$
$$(u-1,\ v+1,\ w+1),\ (u-1,\ v,\ w+1).$$

如此所得的这些立方格必在球

$$u^2+v^2+w^2=(\sqrt{x}+\sqrt{3})^2$$

之中，但同时又包有球

$$u^2+v^2+w^2=(\sqrt{x}-\sqrt{3})^2.$$

因此如果设球

$$u^2+v^2+w^2\leqslant x$$

内整点数为N，则

$$\frac{4}{3}\pi(\sqrt{x}-\sqrt{3})^3\leqslant N\leqslant\frac{4}{3}\pi(\sqrt{x}+\sqrt{3})^3$$

此即　　$N=\frac{4}{3}\pi x^{\frac{3}{2}}+O(x)$.

习题3　试推广上题到n度空间之球

解：用$A_n(x)$记n度空间球

$$u_1{}^2+u_2{}^2+\cdots+u^{\ 2}\leqslant x$$

内的整点数．由提要中定理13可得

$$A_2(x)=\pi x+O(\sqrt{x})=O(x)$$

由习题 2 可得

$$A_3(x)=\frac{4}{3}\pi x^{\frac{3}{2}}+O(x)=O(x^{\frac{3}{2}})$$

另外还有 *

$$A_4(x)=\frac{1}{2}\pi^2x^2+O(x\log^{\frac{3}{4}}x\log\log^{\frac{1}{4}}x)=O(x^2)$$

下面用归纳法证明

---

* $A_4(x)$的表达式请参阅《堆垒素数论》第158页.

$$A_n(x)=O(x^{\frac{n}{2}}),\quad n\geqslant 2 \qquad (1)$$

$n=2$，3，4时见上述可知(1)成立。归纳假定$n=k$时(1)成立，当$n=k+1$时

$$A_{k+1}(x)=\sum_{u_1^2+\cdots u_k^2+u_{k+1}^2\leqslant x}1$$

$$=2\sum_{0\leqslant i\leqslant\sqrt{x}}\ \sum_{u_1^2+\cdots+u_k^2\leqslant x-i^2}1$$

$$=2\sum_{0\leqslant i\leqslant\sqrt{x}}A_k(x-i^2)$$

$$=2\sum_{0\leqslant i\leqslant\sqrt{x}}O\left((x-i^2)^{\frac{k}{2}}\right)$$

$$=\sum_{0\leqslant i\leqslant\sqrt{x}}O(x^{\frac{k}{2}})$$

$$=O\left(x^{\frac{k}{2}}\sum_{0\leqslant i\leqslant\sqrt{x}}1\right)$$

$$=O\left(x^{\frac{k}{2}}([\sqrt{x}]+1)\right)$$

$$=O\left(x^{\frac{k+1}{2}}\right).$$

此即$n=k+1$时(1)仍然成立。

习题4 求出

$$\sum_{1\leqslant n\leqslant x}r^2(n)$$

之无穷大之阶.

解：由提要中定理12知，对任意小的正数$\frac{\varepsilon}{2}>0$，**都有**

$$\sum_{1\leqslant n\leqslant x} r^2(n)=\sum_{1\leqslant n\leqslant x}\left(O(n^{\frac{\varepsilon}{2}})\right)^2$$

$$=\sum_{1\leqslant n\leqslant x} O(n^{\varepsilon})=\sum_{1\leqslant n\leqslant x} O(x^{\varepsilon})$$

$$=O\left(x^{\varepsilon}\sum_{1\leqslant n\leqslant x} 1\right)$$

$$=O(x^{1+\varepsilon}),$$

此即对任给的$\varepsilon>0$，可得

$$\sum_{1\leqslant n\leqslant x} r^2(n)=O(x^{1+\varepsilon}) \qquad (1)$$

另一方面，对于任意的$\varepsilon>0$，下式绝不能成立：

$$\sum_{1\leqslant n\leqslant x} r^2(n)=O(x^{1-\varepsilon})$$

当a_i，b_i（$1\leqslant i\leqslant l$）为实数，从熟知的不等式

$$\left(\sum_{i=1}^{l} a_i^2\right)\left(\sum_{i=1}^{l} b_i^2\right)\geqslant\left(\sum_{i=1}^{l} a_i b_i\right)^2$$

可得 $$\sum_{1\leqslant n\leqslant x} r^2(n)\sum_{1\leqslant n\leqslant x} 1^2\geqslant\left(\sum_{1\leqslant n\leqslant x} r(n)\right)^2$$

$$\sum_{1\leqslant n\leqslant x} r^2(n)\geqslant\frac{1}{x}\left(\sum_{1\leqslant n\leqslant x} r(n)\right)^2 \qquad (2)$$

由于 $$\sum_{1\leqslant n\leqslant x} r(n)=\pi x+O(\sqrt{x})$$

因此可找到常数$A>0$。当x充分大时

$$\sum_{1\leqslant n\leqslant x} r(n)\geqslant\pi x-A\sqrt{x}$$

把上式代入(2)得

$$\sum_{1\leqslant n\leqslant x} r^2(n) \geqslant \pi^2 x - 2\pi A\sqrt{x} + A^2 \tag{3}$$

若存在$\varepsilon>0$，使得

$$\sum_{1\leqslant n\leqslant x} r^2(n) = O(x^{1-\varepsilon})$$

就可以找到常数$B>0$。当x充分大时

$$\sum_{1\leqslant n\leqslant x} r^2(n) \leqslant Bx^{1-\varepsilon} \tag{4}$$

但是当x充分大时，(3)和(4)互相矛盾。

公式(1)可从推广成：对任给的$\varepsilon>0$

$$\sum_{1\leqslant n\leqslant x} r^k(n) = O(x^{1+\varepsilon}),\ k\text{为正整数}.$$

对$\frac{\varepsilon}{k}$使用定理12，便可证明上式．由定理12得

$$\sum_{1\leqslant n\leqslant x} r^k(n) = \sum_{1\leqslant n\leqslant x}\left(O(n^{\frac{\varepsilon}{k}})\right)^k$$

$$= \sum_{1\leqslant n\leqslant x} O(n^{\varepsilon}) = \sum_{1\leqslant n\leqslant x} O(n^{\varepsilon})$$

$$= O(x^{\varepsilon})\sum_{1\leqslant n\leqslant x} 1$$

$$= O(x^{1+\varepsilon}).$$

又： 若用$r(n)$表方程

$$x_1^k + x_2^k + \cdots + x_l^k = n,\quad x_m \geqslant 0$$

的解数，则有下面两个定理

定理1 若$x\geqslant 1$，则

$$\sum_{1\leqslant n\leqslant x} r(n) \geqslant A(k)x^{\frac{l}{k}}.$$

定理2　若$k\geqslant 2$及$x\geqslant 1$，则

$$\sum_{1\leqslant n\leqslant x} r^2(n)\leqslant B(k)x^{\frac{2l}{k}-1}.$$

以上两个定理中，$l=\frac{1}{2}\cdot 8^{k-1}$而$A$、$B$是两个只与$k$有关的常数。它们的证明，可参看第十九章第六节。如果取$k=2$，则有

$$A_4(x)\geqslant Ax^2 \text{和} \sum_{1\leqslant n\leqslant x} r^2(n)\leqslant Bx^3$$

其中$A_4(x)$的定义见习题3，即表四度空间球$u_1^2+u_2^2+u_3^2+u_4^2\leqslant x$内的整点数。

习题5　圆内

$$u^2+v^2\leqslant x$$

之两坐标互素之整点数$=\frac{6}{\pi}x+O(\sqrt{x}\log x)$。

证：设N_d表圆

$$u^2+v^2\leqslant\frac{x}{d^2}$$

内的整点数，N表圆

$$u^2+v^2\leqslant x$$

内两坐标互素的整点数，则由

$$\sum_{d|a}\mu(d)=\begin{cases}1, & 若a=1\\ 0, & 若a>1\end{cases}$$

可得

$$N=\sum_{\substack{u^2+v^2\leqslant x\\(u,v)=1}}1=\sum_{u^2+v^2\leqslant x}\sum_{d|(u,v)}\mu(d)$$

$$=\sum_{1\leqslant d\leqslant\sqrt{x}}\mu(d)\sum_{u^2+v^2\leqslant\frac{x}{d^2}}1=\sum_{1\leqslant d\leqslant\sqrt{x}}\mu(d)N_d$$

又因为 $N_d = \pi\frac{x}{d^2} + O\left(\frac{\sqrt{x}}{d}\right)$

故 $$N = \sum_{1\leqslant d\leqslant\sqrt{x}} \mu(d)\left(\pi\frac{x}{d^2} + O\left(\frac{\sqrt{x}}{d}\right)\right)$$

$$= \pi x \sum_{1\leqslant d\leqslant\sqrt{x}} \frac{\mu(d)}{d^2} + O\left(\sqrt{x} \sum_{1\leqslant d\leqslant\sqrt{x}} \frac{1}{d}\right)$$

$$= \pi x \sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} + O\left(x \sum_{d\geqslant\sqrt{x}} \frac{1}{d^2}\right) + O(\sqrt{x}\log x)$$

$$= \pi x \cdot \frac{6}{\pi^2} + O(\sqrt{x}) + O(\sqrt{x}\log x)$$

$$= \frac{6}{\pi}x + O(\sqrt{x}\log x) .$$

§10 Ferey贯及其应用

习题 证明二邻项之分母不同。

证： 设 $\frac{a}{b}<\frac{a'}{b'}$

为n级Ferdy贯中相邻两项．由提要中定理15得

$$ba' - ab' = 1$$

如果$b = b'$，就有

$$b(a' - a) = 1$$

$$b = b' = 1$$

又因为

$$b + b' \geqslant n + 1,\ n\geqslant 2$$

故 $$2\geqslant 3.$$

此不可能，因此$b \neq b'$。

§14 Dirichlet级数

习题1 讨论式(1)～(9)成立之范围。

$$\zeta(s)=\prod_p\left(1-\frac{1}{p^s}\right)^{-1} \tag{1}$$

$$\frac{1}{\zeta(s)}=\prod_p\left(1-\frac{1}{p^s}\right)=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} \tag{2}$$

$$\zeta^2(s)=\sum_{n=1}^{\infty}\frac{d(n)}{n^s} \tag{3}$$

$$\frac{\zeta(s)}{\zeta(2s)}=\frac{\prod_p\left(1-\frac{1}{p^{2s}}\right)}{\prod_p\left(1-\frac{1}{p^s}\right)}=\prod_p\left(1+\frac{1}{p^s}\right)$$

$$=\sum_{n=1}^{\infty}\frac{|\mu(n)|}{n^s} \tag{4}$$

$$\frac{\zeta'(s)}{\zeta(s)}=-\sum_p\frac{\log p}{p^s}\left(1-\frac{1}{p^s}\right)^{-1}$$

$$=-\sum_p\log p\sum_{m=1}^{\infty}\frac{1}{p^{ms}}=-\sum_{n=2}^{\infty}\frac{\Lambda(n)}{n^s} \tag{5}$$

$$\zeta'(s)=-\sum_{n=2}^{\infty}\frac{\log n}{n^s} \tag{6}$$

$$\log\zeta(s)=-\sum_p\log\left(1-\frac{1}{p^s}\right)=\sum_p\sum_{m=1}^{\infty}\frac{1}{mp^{sm}}$$

$$=\sum_{n=1}^{\infty}\frac{\Lambda_1(n)}{n^s} \tag{7}$$

$$\frac{\zeta''(s)}{\zeta(s)}=\frac{d}{ds}\frac{\zeta'(s)}{\zeta(s)}+\left(\frac{\zeta'(s)}{\zeta(s)}\right)^2 \qquad (8)$$

$$\sum_{n=1}^{\infty}\frac{r(n)}{n^s}=4L(s)\zeta(s) \qquad (9)$$

解：1)　由于$\sum_{n=1}^{\infty}\frac{1}{n^s}$当$s>1$时收敛，故(1)成立范围为$s>1$；

2)由1)可知(2)成立的范围为$s>1$；

3)由于$\zeta^2(s)=\zeta(s)\cdot\zeta(s)$，故(3)成立范围与(1)和(2)相同；

4)由于$\prod_p\left(1\pm\frac{1}{p^s}\right)$收敛的充要条件是$\sum_p\frac{1}{p^s}$收敛，而$\sum_p\frac{1}{p}$发散，故(4)成立范围为$s>1$；

5)由于$\zeta'(s)$和$\frac{1}{\zeta(s)}$的收敛范围与$\zeta(s)$的收敛范围相同，故(5)成立范围为$s>1$；

6)理由同5)，(6)成立范围为$s>1$；

7)由于$\zeta(s)$的收敛范围为$s>1$，且$\zeta(s)>1$，故(7)成立范围为$s>1$；

8)由于$\zeta''(s)$、$\zeta'(s)$的收敛范围和$\zeta(s)$的收敛范围同为$s>1$，故(8)成立范围为$s>1$；

9)由于$L(s)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$当$s>1$时绝对收敛，$\zeta(s)$当$s>1$时收敛，故(9)成立范围为$s>1$。

习题2　建立：

$$\frac{\zeta^3(s)}{\zeta(2s)}=\sum_{n=1}^{\infty}\frac{d(n^2)}{n^s}, \qquad s>1$$

$$\frac{\zeta^4(s)}{\zeta(2s)}=\sum_{n=1}^{\infty}\frac{(d(n))^2}{n^s}, \qquad s>1$$

$$\frac{\zeta(s-1)}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}, \qquad s>2$$

$$\zeta(s)\zeta(s-a)=\sum_{n=1}^{\infty}\frac{\sigma_a(n)}{n^s}, \qquad s>\max(1,\ a+1)$$

$$\frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)}=\sum_{n=1}^{\infty}\frac{\sigma_a(n)\sigma_b(n)}{n^s},$$

$$s>\max(1,\ a+1,\ b+1,\ a+b+1)。$$

证： Ⅰ) $\frac{\zeta^3(s)}{\zeta(2s)}=\sum_{n=1}^{\infty}\frac{d(n^2)}{n^s}$, $s>1$。

为证上式，首先证明

$$\sum_{d|n}|\mu(d)|d\left(\frac{n}{d}\right)=d(n^2)。$$

设

$$n=p_1^{l_1}p_2^{l_2}\cdots p_k^{l_k}$$

由于 $\sum_{d|n}|\mu(d)|d\left(\frac{n}{d}\right)=\sum_{d|p_1\cdots p_k}|\mu(d)|d\left(\frac{n}{d}\right)$

故只需证明

$$\sum_{d|p_1\cdots p_k}|\mu(d)|d\left(\frac{n}{d}\right)=d(n^2)$$

即可．下面用归纳法证明．当$k=1$时，

$$\sum_{d|p_1}|\mu(d)|d\left(\frac{n}{d}\right)=|\mu(1)|d(p_1^{l_1})+|\mu(p_1)|d(p_1^{l_1-1})$$

$$=(l_1+1)+l_1=2l_1+1$$

$$d(n^2)=d(p_1^{2l_1})=2l_1+1$$

故$k=1$时结论成立。设$k\leqslant t-1$时结论亦成立，则当$k=t$时，

$$\sum_{d|p_1\cdots p_t}|\mu(d)|\left(\frac{n}{d}\right)$$

$$=\sum_{d|p_1\cdots p_{t-1}}|\mu(d)|d\left(\frac{n}{d}\right)+\sum_{d|p_1\cdots p_{t-1}}|\mu(p_t d)|\cdot$$

$$d\left(\frac{n}{p_t d}\right)$$

$$=\sum_{d|p_1\cdots p_{t-1}}|\mu(d)|d\left(\frac{p_1^{l_1}\cdots p_t^{l_t}}{d}\right)+\sum_{d|p_1\cdots p_{t-1}}|\mu(p_t)|\cdot$$

$$|\mu(d)|d\left(\frac{p_1^{l_1}\cdots p_t^{l_t}}{p_t d}\right)$$

$$=d(p_t^{l_t})\sum_{d|p_1\cdots p_{t-1}}|\mu(d)|d\left(\frac{p_1^{l_1}\cdots p_{t-1}^{l_{t-1}}}{d}\right)+d(p_t^{l_t-1})$$

$$\sum_{d|p_1\cdots p_{t-1}}|\mu(d)|d\left(\frac{p_1^{l_1}\cdots p_{t-1}^{l_{t-1}}}{d}\right)$$

$$=d(p_t^{l_t})d(p_1^{2l_1}\cdots p_{t-1}^{2l_{t-1}})+d(p_t^{l_t-1})d(p_1^{2l_1}\cdots p_{t-1}^{2l_{t-1}})$$

$$=[d(p_t^{l_t})+d(p_t^{l_t-1})]\,d(p_1^{2l_1}\cdots p_{t-1}^{2l_{t-1}})$$

$$=(2l_t+1)d(p_1^{2l_1}\cdots p_{t-1}^{2l_{t-1}})$$

$$=d(p_t^{2l_t})d(p_1^{2l_1}\cdots p_{t-1}^{2l_{t-1}})$$

$$=d(p_1^{2l_1}\cdots p_t^{2l_t})$$

$$=d(n^2)$$

此即$k=t$时也有

$$\sum_{d|p_1\cdots p_t}|\mu(d)|d\left(\frac{n}{d}\right)=d(n^2)$$

设 $\sum_{n=1}^{\infty}\frac{|\mu(n)|}{n^s}\sum_{m=1}^{\infty}\frac{d(m)}{m^s}=\sum_{k=1}^{\infty}a_k\frac{1}{k^s}$

则 $$a_k=\sum_{d|k}|\mu(d)|d\left(\frac{k}{d}\right)$$

这是因为$\frac{1}{k}$由$\frac{1}{n}$与$\frac{1}{m^s}$相乘而得，即

$$\frac{1}{k^s}=\frac{1}{n^s}\cdot\frac{1}{m^s}$$

从而 $k=nm$。故$\frac{1}{k^s}$的系数a_k等于

$$c_k=\sum_{d|k}|\mu(d)|d\left(\frac{k}{d}\right)$$

所以 $$\frac{\zeta^3(s)}{\zeta(2s)}=\frac{\zeta(s)}{\zeta(2s)}\cdot\zeta^2(s)=\sum_{n=1}^{\infty}\frac{|\mu(n)|}{n^s}\sum_{m=1}^{\infty}\frac{d(m)}{m^s}$$

$$=\sum_{k=1}^{\infty}a_k\frac{1}{k^s}=\sum_{k=1}^{\infty}\frac{1}{k^s}\sum_{d|k}|\mu(d)|d\left(\frac{k}{d}\right)$$

$$=\sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{d|n}|\mu(d)|d\left(\frac{n}{d}\right)=\sum_{n=1}^{\infty}\frac{d(n^2)}{n^s}.$$

I） $$\frac{\zeta^4(s)}{\zeta(2s)}=\sum_{n=1}^{\infty}\frac{(d(n))^2}{n^s},\qquad s>1.$$

首先证明 $$\sum_{d_1|n}d(d_1^2)=(d(n))^2$$

仍然设 $$n=p_1^{l_1}\cdots p_k^{l_k}$$

则 $$\sum_{d_1|n}d(d_1^2)=\sum_{x_1=0}^{l_1}\sum_{x_2=0}^{l_2}\cdots\sum_{x_k=0}^{l_k}d(p_1^{2x_1}p_2^{2x_2}\cdots$$

$$\cdots p_k^{2x_k})=$$

$$=\sum_{x_1=0}^{l_1} d(p_1^{2x_1})\sum_{x_2=0}^{l_2} d(p_2^{2x_2})\cdots\sum_{x_k=0}^{l_k} d(p_k^{2x_k})$$

$$=\sum_{x_1=0}^{l_1}(2x_1+1)\sum_{x_2=0}^{l_2}(2x_2+1)\cdots\sum_{x_k=0}^{l_k}(2x_k+1)$$

$$=[l_1(l_1+1)+(l_1+1)]\cdots[l_k(l_k+1)+(l_k+1)]$$

$$=(l_1+1)^2\cdots(l_k+1)^2$$

$$=[(l_1+1)\cdots(l_k+1)]^2$$

$$=(d(n))^2.$$

设 $\sum_{n=1}^{\infty}\frac{d(n^2)}{n^s}\sum_{m=1}^{\infty}\frac{1}{m^s}=\sum_{k=1}^{\infty}a_k\frac{1}{k^s}$,

由 $\frac{1}{k^s}=\frac{1}{n^s}\cdot\frac{1}{m^s}$, $k=nm$, 可得

$$a_k=\sum_{d_1|k} d(d_1^2)$$

故 $$\frac{\zeta^4(s)}{\zeta(2s)}=\frac{\zeta^3(s)}{\zeta(2s)}\cdot\zeta(s)=\sum_{n=1}^{\infty}\frac{d(n^2)}{n^s}\sum_{m=1}^{\infty}\frac{1}{m^s}$$

$$=\sum_{k=1}^{\infty}a_k\frac{1}{k^s}=\sum_{k=1}^{\infty}\frac{1}{k^s}\sum_{d_1|k}d(d_1^2)$$

$$=\sum_{n=1}^{\infty}\frac{1}{n^s}\sum_{d_1|n}d(d_1^2)=\sum_{n=1}^{\infty}\frac{(d(n))^2}{n^s}.$$

Ⅱ) $$\frac{\zeta(s-1)}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s},\quad s>2.$$

设 $$\sum_{n=1}^{\infty}\frac{n}{n^s}\sum_{m=1}^{\infty}\frac{\mu(m)}{m^s}=\sum_{k=1}^{\infty}a_k\frac{1}{k^s}$$

同样由$\frac{1}{k^s}=\frac{1}{n^s}\cdot\frac{1}{m^s}$，$k=nm$可得

$$a_k=\sum_{d|k}\mu(d)\frac{k}{d}=\varphi(k)$$

故

$$\frac{\zeta(s-1)}{\zeta(s)}=\zeta(s-1)\cdot\frac{1}{\zeta(s)}$$

$$=\sum_{n=1}^{\infty}\frac{1}{n^{s-1}}\sum_{m=1}^{\infty}\frac{\mu(m)}{m^s}$$

$$=\sum_{n=1}^{\infty}\frac{n}{n^s}\sum_{m=1}^{\infty}\frac{\mu(m)}{m^s}$$

$$=\sum_{k=1}^{\infty}a_k\frac{1}{k^s}$$

$$=\sum_{k=1}^{\infty}\frac{\varphi(k)}{k^s}$$

$$=\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}.$$

Ⅳ） $\zeta(s)\zeta(s-a)=\sum_{n=1}^{\infty}\frac{\sigma_a(n)}{n^s}$，$s>\max(1,\ a+1)$。

设 $\sum_{n=1}^{\infty}\frac{1}{n}\sum_{m=1}^{\infty}\frac{m^a}{m^s}=\sum_{k=1}^{\infty}a_k\frac{1}{k^s}$

则用上面相同的方法可得

$$a_k=\sum_{d|k}d^a$$

故 $\zeta(s)\zeta(s-a)=\sum_{n=1}^{\infty}\frac{1}{n}\sum_{m=1}^{\infty}\frac{1}{m^{s-a}}=\sum_{n=1}^{\infty}\frac{1}{n}\sum_{m=1}^{\infty}\frac{m^a}{m^s}$

$$=\sum_{k=1}^{\infty} a \quad \frac{1}{k^s}=\sum_{k=1}^{\infty}\frac{1}{k^s}\ \sum_{d|k} d^a=\sum_{n=1}^{\infty}\frac{1}{n^s}\ \sum_{a|n} d^a=\sum_{n=1}^{\infty}\frac{\sigma_a(n)}{n^s}.$$

V) $$\frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)}=\sum_{n=1}^{\infty}\frac{\sigma_a(n)\sigma_b(n)}{n^s},$$

$$s>\max(1,\ a+1,\ b+1, a+b+1).$$

$$\frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)}$$

$$=\prod_p\left(1-\frac{1}{p^s}\right)^{-1}\prod_p\left(1-\frac{p^a}{p^s}\right)^{-1}\prod_p\left(1-\frac{p^b}{p^s}\right)^{-1}\cdot$$

$$\cdot\prod_p\left(1-\frac{p^{a+b}}{p^s}\right)^{-1}\prod_p\left(1-\frac{p^{a+b}}{p^{2s}}\right)$$

$$=\prod_p\left(1-\frac{1}{p^s}\right)^{-1}\left(1-\frac{p^a}{p^s}\right)^{-1}\left(1-\frac{p^b}{p^s}\right)^{-1}$$

$$\cdot\left(1-\frac{p^{a+b}}{p^s}\right)^{-1}\left(1-\frac{p^{a+b}}{p^{2s}}\right)$$

$$=\prod_p\left(\sum_{n=0}^{\infty}\frac{1}{p^{ns}}\right)\left(\sum_{n=0}^{\infty}\frac{p^{na}}{p^{ns}}\right)\left(\sum_{n=0}^{\infty}\frac{p^{nb}}{p^{ns}}\right)\left(\sum_{n=0}^{\infty}\frac{p^{n(a+b)}}{p^{ns}}\right)$$

$$\cdot\left(1-\frac{p^{a+b}}{p^{2s}}\right). \tag{1}$$

设$x=p^{-s}$，则由乘法公式得

$$\left(\sum_{n=0}^{\infty}\frac{1}{p^{ns}}\right)\left(\sum_{n=0}^{\infty}\frac{p^{n(a+b)}}{p^{ns}}\right)$$

$$=\left(\sum_{n=0}^{\infty}x^n\right)\left(\sum_{n=0}^{\infty}p^{n(a+b)}x^n\right)=\sum_{n=0}^{\infty}a_n\,x^n$$

其中

$$a_n = 1 + p^{a+b} + \cdots + p^{n(a+b)}$$

$$\left(\sum_{n=0}^{\infty}\frac{p^{na}}{p^{ns}}\right)\left(\sum_{n=0}^{\infty}\frac{p^{nb}}{p^{ns}}\right) = \left(\sum_{n=0}^{\infty}p^{na}x^n\right)\left(\sum_{n=0}^{\infty}p^{nb}x^n\right)$$

$$= \sum_{n=0}^{\infty} b_n x^n$$

其中 $b_0 = 1$

$$b_n = p^{na} + p^{(n-1)a}p^b + \cdots + p^a p^{(n-1)b} + p^{nb}, \quad n \geqslant 1$$

$$\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty} C_n x^n$$

其中 $C_n = a_n b_0 + a_{n-1}b_1 + \cdots + a_0 b_n$

故 $$\left(\sum_{n=0}^{\infty}\frac{1}{p^{ns}}\right)\left(\sum_{n=0}^{\infty}\frac{p^{na}}{p^{ns}}\right)\left(\sum_{n=0}^{\infty}\frac{p^{nb}}{p^{ns}}\right)\left(\sum_{n=0}^{\infty}\frac{p^{n(a+b)}}{p^{ns}}\right)$$

$$\cdot\left(1 - \frac{p^{a+b}}{p^{2s}}\right)$$

$$= \left(\sum_{n=0}^{\infty} C_n x^n\right)\left(1 - p^{a+b}x^2\right)$$

$$= \sum_{n=0}^{\infty} C_n x^n - p^{a+b}\sum_{n=0}^{\infty} C_n x^{n+2}$$

$$= C_0 + C_1 x + \sum_{n=2}^{\infty} C_n x^n - p^{a+b}\sum_{n=2}^{\infty} C_{n-2}x^n$$

$$= C_0 + C_1 x + \sum_{n=2}^{\infty}\left(C_n - p^{a+b}C_{n-2}\right)x^n \tag{2}$$

下面将借助两个引理来证明$n \geqslant 2$时，

$$C_n - p^{a+b}C_{n-2} = \sigma_a(p^n)\sigma_b(p^n). \tag{3}$$

引理1 当$k \geqslant 0$时：

$$b_{k+2}-p^{a+b}b_k=p^{(k+2)a}+p^{(k+2)b}.$$

当$k=0$时：$b_0=1$，

$$b_{k+2}-p^{a+b}b_k=b_2-p^{a+b}b_0$$

$$=p^{2a}+p^{a+b}+p^{2b}-p^{a+b}=p^{2a}+p^{2b}$$

当$k\geqslant 1$时：

$$b_k=p^{ka}+p^{(k-1)a}p^b+\cdots\cdots+p^a p^{(k-1)b}+p^{kb},$$

$$b_{k+2}-p^{a+b}b_k$$

$$=p^{(k+2)a}+p^{(k+1)a}p^b+\cdots+p^a p^{(k+1)b}+p^{(k+2)b}-$$

$$-p^{(k+1)a}p^b-\cdots-p^a p^{(k+1)b}$$

$$=p^{(k+2)a}+p^{(k+2)b}$$

引理2　当$k\geqslant 0$时

$$p^{k(a+b)}(p^{a+b}-1)b_0+p^{(k-1)(a+b)}(p^{a+b}-1)b_1+$$

$$+p^{(k-2)(a+b)}(p^{a+b}-1)b_2+\cdots+p^{2(a+b)}(p^{a+b}-1)b_{k-2}+$$

$$+p^{(a+b)}(p^{a+b}-1)b_{k-1}+p^{a+b}b_k+b_{k+1}=$$

$$=p^{(k+1)a}(1+p^b+\cdots+p^{kb})+$$

$$+p^{(k+1)b}(1+p^a+\cdots+p^{ka})+p^{(k+1)(a+b)}$$

当$k=0$时上式

左端$=p^{a+b}b_0+b_1=p^{a+b}+p^a+p^b$

右端$=p^a+p^b+p^{a+b}$

因此$k=0$时引理2成立。设$k=t$时亦成立，则当$k=t+1$时

$$p^{(t+1)(a+b)}(p^{a+b}-1)b_0+p^{t(a+b)}(p^{a+b}-1)b_1+$$

$$+p^{(t-1)(a+b)}(p^{a+b}-1)b_2+\cdots+p^{3(a+b)}(p^{a+b}-1)b_{t-2}+$$

$$+p^{2(a+b)}(p^{a+b}-1)b_{t-1}+p^{(a+b)}(p^{a+b}-1)b_t+$$

$$+p^{a+b}b_{t+1}+b_{t+2}$$

$$=p^{a+b}\{p^{t(a+b)}(p^{a+b}-1)b_0+p^{(t-1)(a+b)}(p^{a+b}-1)b_1+$$

$$+p^{(t-2)(a+b)}(p^{a+b}-1)b_2+\cdots+p^{2(a+b)}(p^{a+b}-1)b_{t-2}+$$

$$+p^{a+b}(p^{a+b}-1)b_{t-1}+(p^{a+b}-1)b_t+b_{t+1}\}+b_{t+2}$$

$$=p^{a+b}\{p^{(t+1)a}(1+p^b+\cdots+p^{tb})+$$

$$+p^{(t+1)b}(1+p^a+\cdots+p^{ta})+p^{(t+1)(a+b)}-b_t\}+$$
$$+b_{t+2}$$
$$=p^{a+b}\{p^{(t+1)a}(1+p^b+\cdots+p^{tb})+$$
$$+p^{(t+1)b}(1+p^a+\cdots+p^{ta})\}+p^{(t+2)(a+b)}+$$
$$+b_{t+2}-p^{a+b}b_t$$
$$=p^{(t+2)a}(p^b+\cdots+p^{(t+1)b})+$$
$$+p^{(t+2)b}(p^a+\cdots+p^{(t+1)a})+p^{(t+2)(a+b)}+$$
$$+p^{(t+2)a}+p^{(t+2)b}$$
$$=p^{(t+2)a}(1+p^b+\cdots+p^{(t+1)b})+$$
$$+p^{(t+2)b}(1+p^a+\cdots+p^{(t+1)a})+p^{(t+2)(a+b)}$$

此即$k=t+1$时结论仍然成立，故引理 2 是成立的。

现在证明$n\geqslant 2$时

$$C_n-p^{a+b}C_{n-2}=\sigma_a(p^n)\sigma_b(p^n) \tag{3}$$

使用归纳法。$n=2$时

$$C_2-p^{a+b}C_0=a_2b_0+a_1b_1+a_0b_2-p^{a+b}\cdot 1$$
$$=(1+p^{a+b}+p^{2(a+b)})\cdot 1+(1+p^{a+b})(p^a+p^b)+$$
$$+1\cdot(p^{2a}+p^{a+b}+p^{2b})-p^{a+b}$$
$$=(1+p^a+p^{2a})(1+p^b+p^{2b})=\sigma_a(p^2)\sigma_b(p^2),$$

因此$n=2$时(3)成立。设$n=k$时(3)亦成立，即

$$C_k-p^{a+b}C_{k-2}=\sigma_a(p^k)\sigma_b(p^k). \tag{3'}$$

则当$n=k+1$时，因为

$$C_{k+1}=a_{k+1}b_0+a_kb_1+\cdots+a_2b_{k-1}+a_1b_k+a_0b_{k+1}$$
$$=(1+p^{a+b}+\cdots+p^{k(a+b)}+p^{(k+1)(a+b)})b_0+$$
$$+(1+p^{a+b}+\cdots+p^{(k-1)(a+b)}+p^{k(a+b)})b_1+\cdots$$
$$+(1+p^{a+b}+p^{2(a+b)})b_{k-1}+$$
$$+(1+p^{a+b})b_k+$$
$$+b_{k+1}$$
$$=a_kb_0+p^{(k+1)(a+b)}b_0+$$

$$+a_{k-1}b_1+p^{k(a+b)}b_1+\cdots$$
$$+\cdots\quad+\cdots$$
$$+a_1b_{k-1}+p^{2(a+b)}b_{k-1}+$$
$$+a_0b_k+p^{a+b}b_k+$$
$$+b_{k+1}$$
$$=C_k+p^{(k+1)(a+b)}b_0+p^{k(a+b)}b_1+\cdots+$$
$$+p^{2(a+b)}b_{k-1}+p^{a+b}b_k+b_{k+1}\qquad(4)$$

同理 $C_{k-1}=C_{k-2}+p^{(k-1)(a+b)}b_0+p^{(k-2)(a+b)}b_1+\cdots+$
$$+p^{2(a+b)}b_{k-3}+p^{a+b}b_{k-2}+b_{k-1}\qquad(5)$$

故将(4)、(5)代入(3′)得

$$C_{k+1}-(p^{(k+1)(a+b)}b_0+p^{k(a+b)}b_1+\cdots+$$
$$+p^{2(a+b)}b_{k-1}+p^{a+b}b_k+b_{k+1})-$$
$$-p^{a+b}(C_{k-1}-p^{(k-1)(a+b)}b_0-p^{(k-2)(a+b)}b_1-\cdots-$$
$$-p^{2(a+b)}b_{k-3}-p^{a+b}b_{k-2}-b_{k-1})$$
$$=\sigma_a(p^k)\sigma_b(p^k)$$

即 $C_{k+1}-p^{a+b}C_{k-1}=\sigma_a(p^k)\sigma_b(p^k)+p^{k(a+b)}(p^{a+b}-1)b_0+$
$$+p^{(k-1)(a+b)}(p^{a+b}-1)b_1+\cdots+p^{2(a+b)}(p^{a+b}-1)b_{k-2}+$$
$$+p^{(a+b)}(p^{a+b}-1)b_{k-1}+p^{a+b}b_k+b_{k+1}$$

由引理2立刻得到

$$C_{k+1}-p^{a+b}C_{k-1}$$
$$=\sigma_a(p^k)\sigma_b(p^k)+p^{(k+1)a}(1+p^b+\cdots+p^{kb})+$$
$$+p^{(k+1)b}(1+p^a+\cdots+p^{ka})+p^{(k+1)(a+b)}\qquad(6)$$

再把 $\sigma_a(p^k)\sigma_b(p^k)=(1+p^a+\cdots+p^{ka})(1+p^b+\cdots+p^{kb})$

代入(6)就得

$$C_{k+1}-p^{a+b}C_{k-1}=(1+p^a+\cdots+p^{(k+1)a})(1+p^b+\cdots$$
$$+p^{(k+1)b})=\sigma_a(p^{k+1})\sigma_b(p^{k+1}),$$

故$n=k+1$时(3)仍然成立。把(3)、(2)代入(1)，且注意到$x=p^{-s}$，就有

$$\frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)}$$

$$=\prod_p\left(C_0+C_1\frac{1}{p^s}+\sum_{n=2}^{\infty}\sigma_a(p^n)\sigma_b(p^n)\frac{1}{p^{ns}}\right)$$

又易知　$C_0=1$

$$C_1=1+p^a+p^b+p^{a+b}=(1+p^a)(1+p^b)$$
$$=\sigma_a(p)\sigma_b(p),$$

所以　$\frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)}$

$$=\prod_p\left(1+\sigma_a(p)\sigma_b(p)\frac{1}{p^s}+\sigma_a(p^2)\sigma_b(p^2)\frac{1}{p^{2s}}+\cdots\right)$$

最后，设

$$\prod_p\left(1+\sigma_a(p)\sigma_b(p)\frac{1}{p^s}+\sigma_a(p^2)\sigma_b(p^2)\frac{1}{p^{2s}}+\cdots\right)$$

$$=\sum_{n=1}^{\infty}\frac{A_n}{n^s}$$

且设　$n=p_1^{l_1}p_2^{l_2}\cdots p_t^{l_t}$

显然　$\frac{A_n}{n^s}=\sigma_a(p_1^{l_1})\sigma_b(p_1^{l_1})\frac{1}{p_1^{l_1s}}\cdot\sigma_a(p_2^{l_2})\sigma_b(p_2^{l_2})$

$$\frac{1}{p_2^{l_2s}}\cdot\cdots$$

$$\cdot\sigma_a(p_t^{l_t})\sigma_b(p_t^{l_t})\frac{1}{p_t^{l_ts}}$$

$$=\frac{\sigma_a(p_1^{l_1})\cdots\sigma_a(p_t^{l_t})\sigma_b(p_1^{l_1})\cdots\sigma_b(p_t^{l_t})}{p_1^{l_1s}\cdots p_t^{l_ts}}$$

再从$\sigma_a(n)$，$\sigma_b(n)$为积性函数就得到

$$\frac{A_n}{n^s}=\frac{\sigma_a(n)\sigma_b(n)}{n^s}$$

此即 $A_n=\sigma_a(n)\sigma_b(n)$

故

$$\frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)}=\sum_{n=1}^{\infty}\frac{\sigma_a(n)\sigma_b(n)}{n^s}.$$

第七章　三角和及特征

一、提　　要

定理 1

$$\frac{1}{m}\sum_{a=0}^{m-1} e^{2\pi i a n/m} = \begin{cases} 1, & 若m|n, \\ 0, & 若m\nmid n. \end{cases}$$

定义　对模m的一个特征$\chi(n)$是一个仅当$(n,m)=1$时有定义的函数且$\chi(n)$适合：

1）$\chi(1)\neq 0$；

2）若$a\equiv b(\bmod m)$，则$\chi(a)=\chi(b)$；

3）$\chi(ab)=\chi(a)\chi(b)$．

定义　用χ_0表特征$\chi(n)=1$，称为主特征．

定理 2

$$\sum_{n=1}^{m}\chi(n)=\begin{cases}\varphi(m), & 若\chi=\chi_0 \\ 0, & 若\chi\neq\chi_0\end{cases}$$

$$\sum_{\chi}\chi(n)=\begin{cases}\varphi(m), & 若n\equiv 1(\bmod m) \\ 0, & 若n\not\equiv 1(\bmod m)\end{cases}$$

定理 3　命

$$C_q(n)=\sum_{(a,q)=1} e^{2\pi i a n/q}$$

此处a过模q的一个缩系，则

1）$C_q(n)$对q是积性函数，即若$(q_1, q_2)=1$，则

$$C_{q_1}(n)C_{q_2}(n)=C_{q_1q_2}(n)$$

2）
$$C_{p^l}(n)=\begin{cases}p^l-p^{l-1}, & 若p^l\mid n\\ -p^{l-1}, & 若p^{l-1}\| n\\ 0, & 若p^{l-1}\nmid n\end{cases}$$

3）
$$C_q(1)=\mu(q)$$

定义 三角和

$$S(n, m)=\sum_{x=0}^{m-1}e^{2\pi i x^2 n/m}, (n, m)=1$$

称为Causs和。

定理 4 若m是奇数，则

$$S(n, m)=\begin{cases}\left(\frac{n}{m}\right)\sqrt{m}, & 若m\equiv 1(\bmod 4)\\ i\left(\frac{n}{m}\right)\sqrt{m}, & 若m\equiv 3(\bmod 4)\end{cases}$$

定理 5 设p为素数，$d p-1$，整数x为d次非剩余，mod$p$的必要且充分条件为

$$\frac{1}{d}\sum_{a=1}^{d}e^{2\pi i a \operatorname{ind} x/d}=0$$

不然，则此式等于1。

定理 6 命$d=(k, p-1)$，则

$$\left|\sum_{x=1}^{p}e^{2\pi i a x^k/p}\right|\leqslant (d-1)\sqrt{p}.$$

定理 7 命

$$f(x)=a_k x^k+\cdots a_1x+a_0$$

为一整系数多项式，若

$$(a_k, \cdots, a_0, q)=1,$$

则 $$S(q,\ f(x))=\sum_{x=1}^{q}e^{2\pi i f(x)/q}$$

$$=O\left(q^{1-\frac{1}{k}+\varepsilon}\right)$$

此处ε为任给的正数，O中包含的常数只与k及ε有关。

二、题　　解

§1　剩余系之表示法

习题 1　设 $(n,\ m)=1$，

$$S=\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}\xi(x)\eta(y)e^{2\pi ixyn/m}$$

$$\sum_{x=0}^{m-1}|\xi(x)|^2=X_0,\quad \sum_{y=0}^{m-1}|\eta(y)|^2=Y_0,$$

则

$$|S|\leqslant\sqrt{X_0Y_0m}.$$

证：因为

$$S=\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}\xi(x)\eta(y)\,e^{2\pi ixyn/m}$$

$$\bar{S}=\sum_{x=0}^{m-1}\sum_{y_1=0}^{m-1}\bar{\xi}(x)\,\bar{\eta}(y_1)\ e^{-2\pi ixy_1n/m}$$

所以 $$|S|^2=S\cdot\bar{S}\leqslant$$

$$\leqslant \sum_{x=0}^{m-1} \xi(x)\overline{\xi(x)} \sum_{x=0}^{m-1} \sum_{y=0}^{m-1} \sum_{y_1=0}^{m-1} \eta(y)\overline{\eta(y_1)} e^{2\pi i x(y-y_1)n/m}$$

$$= X_0 \sum_{x=0}^{m-1} \sum_{y=0}^{m-1} \sum_{y_1=0}^{m-1} \eta(y)\overline{\eta(y_1)} e^{2\pi i x(y-y_1)n/m}.$$

又因 $\displaystyle\sum_{x=0}^{m-1} \eta(y)\overline{\eta(y_1)} e^{2\pi i x(y-y_1)n/m}$

$$= \eta(y)\overline{\eta(y_1)} \sum_{x=0}^{m-1} e^{2\pi i x(y-y_1)n/m}$$

$$= \begin{cases} |\eta(y)|^2 m, & \text{若} y = y_1 \\ 0, & \text{若} y \neq y_1 \end{cases}$$

从而 $\displaystyle\sum_{x=0}^{m-1} \sum_{y=0}^{m-1} \sum_{y_1=0}^{m-1} \eta(y)\eta(\overline{y_1}) e^{2\pi i x(y-y_1)n/m}$

$$= m \sum_{y=0}^{m-1} |\eta(y)|^2 = mY_0$$

故

$$|S| \leqslant \sqrt{X_0 Y_0 m}.$$

§2 特征函数

习题1 若$\chi \neq \chi_0$，则对任意的正整数u和v $(v \geqslant u)$，有

$$\left|\sum_{n=u}^{v} \chi(n)\right| \leqslant \frac{\varphi(m)}{2}.$$

证：设

$$v - u = qm + r, \quad 0 \leqslant r \leqslant m-1$$

1) 当$r = 0$时：

$$\sum_{n=u}^{v} \chi(n) = q \sum_{n=1}^{m} \chi(n)$$

由提要中定理 2 知道 $$\sum_{n=1}^{m}\chi(n)=0$$

故 $$\sum_{n=u}^{v}\chi(n)=q\cdot 0=0$$

此时结论成立。

ii）当 $1\leqslant r\leqslant m-1$ 时：

因为 $$\sum_{n=u}^{v}\chi(n)=q\sum_{n=1}^{m}\chi(n)+\sum_{n=1}^{r}\chi(n)=\sum_{n=1}^{r}\chi(n)$$

且 $$\left|\sum_{n=1}^{r}\chi(n)\right|+\sum_{n=r+1}^{m}\left|\chi(n)\right|\leqslant\sum_{n=1}^{r}\left|\chi(n)\right|+\sum_{n=r+1}^{m}\left|\chi(n)\right|\leqslant\varphi(m)$$

又因为 $$\sum_{n=1}^{r}\chi(n)=\sum_{n=1}^{m}\chi(n)-\sum_{n=r+1}^{m}\chi(n)=-\sum_{n=r+1}^{m}\chi(n)$$

$$\left|\sum_{n=1}^{r}\chi(n)\right|=\left|\sum_{n=r+1}^{m}\chi(n)\right|$$

从而 $$\left|\sum_{n=1}^{r}\chi(n)\right|\leqslant\frac{\varphi(m)}{2}$$

故 $$\left|\sum_{n=u}^{v}\chi(n)\right|\leqslant\frac{\varphi(m)}{2}$$

习题 2 若 $(l,\ m)=1$，则

$$\sum_{\chi}\frac{(\chi n)}{\chi(l)}=\begin{cases}\varphi(m), & 当 n\equiv l(\bmod m)\\ 0, & 当 n\not\equiv l(\bmod m)\end{cases}$$

证： 因为$\dfrac{\chi(n)}{\chi(l)}$仍然是特征，故有

$$\sum_{\chi}\frac{\chi(n)}{\chi(l)}=\sum_{\chi}\frac{\chi(nl_1)}{\chi(ll_1)}$$

由于 $(l, m)=1$， 故可取l_1，使之其合条件

$$ll_1\equiv 1 \pmod{m}$$

此时 $\sum_{\chi}\frac{\chi(n)}{\chi(l)}=\sum_{\chi}\frac{\chi(nl_1)}{\chi(ll_1)}=\sum_{\chi}\frac{(nl_1)}{\chi(1)}=\sum_{\chi}\chi(nl_1)$

由提要中定理2

$$\sum_{\chi}\chi(k)=\begin{cases}\varphi(m), & 当k\equiv 1 \pmod{m}\\ 0, & 当k\not\equiv 1 \pmod{m}\end{cases}$$

可知，当$nl_1\equiv 1 \pmod{m}$，即$n\equiv l \pmod{m}$ 时

$$\sum_{\chi}\chi(nl_1)=\varphi(m)$$

亦即

$$\sum_{\chi}\frac{\chi(n)}{\chi(l)}=\varphi(m)$$

而 $nl_1\not\equiv 1 \pmod{m}$，即$n\not\equiv l \pmod{m}$ 时

$$\sum_{\chi}\chi(nl_1)=0$$

亦即

$$\sum_{\chi}\frac{\chi(n)}{\chi(l)}=0$$

所以

$$\sum_{\chi}\frac{\chi(n)}{\chi(l)}=\begin{cases}\varphi(m), & 当n\equiv l \pmod{m}\\ 0, & 当n\not\equiv l \pmod{m}\end{cases}$$

§6 特征和三角和

习题 仿定理5·1及5.2以研究三角和

$$\sum_{x=0}^{m-1}e^{2\pi i x^k n/m},\quad (n, m)=1$$

解： $k=2$ 时就是Gauss和，故取$k\geqslant 3$。

设 $$S(n,\ m)=\sum_{x=0}^{m-1}e^{2\pi i x^k n/m}$$

下面证明 $|S(n,\ m)|<cm^{1-\frac{1}{k}}$

此处 $c=k^{6k^6+k}$。

1）如果 $(k,\ p-1)=p$，由提要中定理6可得

$$|S(n,\ p)|\leqslant(d-1)\sqrt{p}$$

2）设 $(k,\ p)=1$，s是整数且 $1<s\leqslant k$，则

$$S(n,p^s)=p^{s-1}$$

而设 $x=u+p^{s-1}v$，$u=0$，…，$p^{s-1}-1$；

$$v=0，\cdots，p-1$$

则 $$e^{2\pi i x^k n/p^s}=e^{2\pi i n(u^k p^{-s}+ku^{k-1}p^{-1}v)}$$

故 $$S(n,\ p^s)=\sum_{x=0}^{p^s-1}e^{2\pi i x^k n/p^s}$$

$$=\sum_{u=0}^{p^{s-1}-1}\ \sum_{v=0}^{p-1}e^{2\pi i n(u^k p^{-s}+ku^{k-1}p^{-1}v)}$$

$$=\sum_{\substack{u=0\\ p\nmid u}}^{p^{s-1}-1}\ \sum_{v=0}^{p-1}e^{2\pi i n(u^k p^{-s}+ku^{k-1}p^{-1}v)}$$

$$+\sum_{\substack{u=0\\ p\mid u}}^{p^{s-1}-1}\ \sum_{v=0}^{p-1}e^{2\pi i n(u^k p^{-s}+ku^{k-1}p^{-1}v)}$$

$$=\sum_{\substack{u=0\\ p\nmid u}}^{p^{s-1}-1}e^{2\pi i u^k n/p^s}\sum_{v=0}^{p-1}e^{2\pi i nku^{k-1}v/p}+$$

$$\sum_{\substack{u=1\\p\mid u}}^{p^{s-1}}\sum_{v=1}^{p} e^{2\pi in(u^k p^{-s}+ku^{k-1}p^{-1}v)}$$

又因为$p\nmid nku^{k-1}$时，

$$\sum_{v=0}^{p-1} e^{2\pi inku^{k-1}v/p}=0,$$

从而

$$S(n,\ p^s)=\sum_{\substack{u=1\\p\mid u}}^{p^{s-1}}\sum_{v=1}^{p} e^{2\pi in(u^k p^{-s}+ku^{k-1}p^{-1}v)}$$

$$=\sum_{u=1}^{p^{s-2}}\sum_{v=1}^{p} e^{2\pi in[(pu)^k p^{-s}+(pu)^{k-1}p^{-1}v]}$$

$$=\sum_{u=1}^{p^{s-2}}\sum_{v=1}^{p} e^{2\pi in[u^k p^{k-s}+ku^{k-1}vp^{k-2}]}$$

由 $1<s\leqslant k$，$k\geqslant 3$ 可知，$u^k p^{k-s}+ku^{k-1}vp^{k-2}$ 是整数，故

$$S(n,\ p^s)=\sum_{u=1}^{p^{s-2}}\sum_{v=1}^{p}1=p^{s-2}\cdot p=p^{s-1}.$$

3）设s是整数且$s>k$，则

$$S(n,\ p^s)=p^{k-1}S(n,\ p^{s-k})$$

设$p^\tau\| k$，显然$s\geqslant\tau+3$；

设 $x=u+p^{s-1-\tau}v$，$u=0,\ \cdots,\ p^{s-1-\tau}-1$；

$v=0,\ \cdots,\ p^{\tau+1}-1$

可得 $e^{2\pi ix^k u/p^s}=e^{2\pi in(u^k p^{-s}+ku^{k-1}p^{-1-\tau}v)}$

从而

$$S(n,\ p^s)=\sum_{x=0}^{p^s-1}e^{2\pi ix^k n/p^s}$$

$$=\sum_{u=0}^{p^{s-1-\tau}}\sum_{v=0}^{p^{\tau+1}-1} e^{2\pi in(u^k p^{-s}+ku^{k-1}p^{-1-\tau}v)}$$

$$=\sum_{\substack{u=0\\ p\nmid u}}^{p^{s-1-\tau}-1}\sum_{v=0}^{p^{\tau+1}-1} e^{2\pi in(u^k p^{-s}+ku^{k-1}p^{-1-\tau}v)}$$

$$=\sum_{\substack{u=0\\ p\mid u}}^{p^{s-1-\tau}-1}\sum_{v=0}^{p^{\tau+1}-1} e^{2\pi in(u^k p^{-s}+ku^{k-1}p^{-1-\tau}v)}$$

$$=\sum_{\substack{u=0\\ p\nmid u}}^{p^{s-1-\tau}-1} e^{2\pi iu^k n/p^s}\sum_{v=0}^{p^{\tau+1}-1} e^{2\pi inku^{k-1}v/p^{\tau+1}}$$

$$+\sum_{\substack{u=0\\ p\mid u}}^{p^{s-1-\tau}-1}\sum_{v=0}^{p^{\tau+1}-1} e^{2\pi in(u^k p^{-s}+ku^{k-1}p^{-1-\tau}v)}$$

又因为$p^{\tau+1}\nmid nku^{k-1}$时，

$$\sum_{v=0}^{p^{\tau+1}-1} e^{2\pi inku^{k-1}v/p^{\tau+1}}=0$$

故有 $$S(n,\ p^s)=\sum_{\substack{u=1\\ p\mid u}}^{p^{s-1-\tau}}\sum_{v=1}^{p^{\tau+1}} e^{2\pi in(u^k p^{-s}+ku\,p^{k-1}p^{-1-\tau}v)}$$

$$=\sum_{u=1}^{p^{s-2-\tau}}\sum_{v=1}^{p^{\tau+1}} e^{2\pi in[(pu)^k p^{-s}+k(pu)^{k-1}p^{-1-\tau}v]}$$

$$= \sum_{u=1}^{p^{s-2-\tau}} e^{2\pi i n (pu)^k / p^s} \sum_{v=1}^{p^{\tau+1}} e^{2\pi i n k (pu)^{k-1} v / p^{\tau+1}}$$

$$= \sum_{u=1}^{p^{s-2-\tau}} e^{2\pi i u^k n / p^{s-k}} \cdot p^{\tau+1}$$

$$= p^{\tau+1} \cdot \frac{p^{s-2-\tau}}{p^{s-k}} \cdot \sum_{u=1}^{p^{s-k}} e^{2\pi i u^k n / p^{s-k}}$$

$$= p^{k-1} S(n, p^{s-k}).$$

4）设 $m = p_1^{a_1} \cdots p_t^{a_t} = p_1^{a_1} M_1 = \cdots = p_t^{a_t} M_t$

$p_1 < \cdots < p_t$，且合条件

$n \equiv n_1 M_1 + \cdots + n_t M_t \pmod{m}$

则 $S(n, m) = S(n_1, p_1^{a_1}) \cdots\cdots S(n_t, p_t^{a_t})$.

因为 $\left\{ \dfrac{n_1 M_1 x^k + \cdots + n_t M_t x^k}{m} \right\} = \left\{ \dfrac{n_1 x^k}{p_1^{a_1}} + \cdots + \dfrac{n_t x^k}{p_t^{a_t}} \right\}$

$$= \left\{ \frac{n_1 x_1^k}{p_1^{a_1}} + \cdots + \frac{n_t x_t^k}{p_t^{a_t}} \right\} \quad 0 \leqslant x_i \leqslant p_i^{a_i} - 1, \ 1 \leqslant i \leqslant t$$

且 $e^{2\pi i \frac{n_1 M_1 x^k + \cdots + n_t M_t x^k}{m}}$

$$= e^{2\pi i \left\{ \frac{n_1 M_1 x^k + \cdots + n_t M_t x^k}{m} \right\}},$$

因此 $S(n, m) = \sum_{x=0}^{m-1} e^{2\pi i x^k n / m}$

$$= \sum_{x=0}^{m-1} e^{2\pi i x^k (n_1 M_1 + \cdots + n_t M_t) / m}$$

$$= \sum_{x=0}^{m-1} e^{2\pi i (n_1 M_1 x^k + \cdots + n_t M_t x^k) / m}$$

$$=\sum_{x_1=0}^{p_1^{a_1}-1} e^{2\pi i x_1^k n_1/p_1^{a_1}} \cdots \sum_{x_t=0}^{p_t^{a_t}-1} e^{2\pi i x_t n_t/p_t^{a_t}}$$

$$=S(n_1,\ p_1^{a_1})\cdots S(n_t,\ p_t^{a_t})$$

5）设$T(n,\ m)=m^{-1+v}S(n,\ m)$，$v=\frac{1}{k}$，则

$$T(n,\ m)=T(n_1,\ p_1^{a_1})\cdots T(n_t,\ p_t^{a_t}).$$

因为$m^{-1+v}=(p_1^{a_1}\cdots p_t^{a_t})^{-1+v}$

$$=(p_1^{a_1})^{-1+v}\cdots(p_t^{a_t})^{-1+v}$$

$$S(n,\ m)=S(n_1,\ p_1^{a_1})\cdots S(n_t,\ p_t^{a_t})$$

故 $$T(n,\ m)=(p_1^{a_1})^{-1+v}S(n_1,\ p_1^{a_1})\cdots(p_t^{a_t})^{-1+v}S(n_t,p_t^{a_t})$$

$$=T(n_1,\ p_1^{a_1})\cdots T(n_t,\ p_t^{a_t}).$$

由1）～5）知道：

Ⅰ）$s=1$时，

$$|T(n,\ p^s)|<p^{-1+v}k\sqrt{p}\leqslant kp^{-\frac{1}{6}}.$$

Ⅱ）$2\leqslant s\leqslant k$，$(k,\ p)=1$时，

$$|T(n,\ p^s)|=p^{-s+sv}p^{s-1}\leqslant 1.$$

Ⅲ）$2\leqslant s\leqslant k,(k,p)=p$时，

$$|T(n,\ p^s)|\leqslant p^{-s+sv}p^s\leqslant p\leqslant k.$$

Ⅳ）$s>k$时，由

$$T(n,\ p^s)=p^{-s+sv}p^{k-1}S(n,\ p^{s-k})$$

$$=T(n,\ p^{s-k})$$

知其可以化成$s\leqslant k$的情形。

所以，当$a_1=\cdots=a_t$，即$m=p_1\cdots p_t$，且

$$|T(n_1,\ p_1)|\geqslant 1,\ \cdots\cdots,\ |T(n_t,\ p_t)|\geqslant 1$$

时，Ⅰ）给出

$$|T(n,\ m)| = |T(n_1,\ p_1)|\cdots|T(n_t,\ p_t)|$$
$$\leqslant |T(n_1,\ p_1)|^6\cdots|T(n_t, p_t)|^6$$
$$<(kp_1^{-\frac{1}{6}})^6\cdots(kp_t^{-\frac{1}{6}})^6$$
$$=\frac{k^{6t}}{p_1\cdots p_t}\leqslant\frac{k^{6t}}{t!} \qquad (1)$$

再来证 $$\frac{k^{6t}}{t!}\leqslant k^{6k^6}. \qquad (2)$$

当$t\leqslant k^6$时，（2）显然成立；当 $t\geqslant k^6+1$时，用归纳法证明。$=k^6+1$时，

$$\frac{k^{6t}}{t!}=\frac{k^{6(k^6+1)}}{(k^6+1)!}<\frac{k^{6(k^6+1)}}{k^6}=k^{6k^6}.$$

归纳假定$t=T>k^6+1$时（2）成立，则$t=T+1$时，

$$\frac{k^{6t}}{t!}=\frac{k^{6(T+1)}}{(T+1)!}=\frac{k^6}{T+1}\cdot\frac{k^{6T}}{T!}$$
$$<\frac{k^6}{T+1}\cdot k^{6k^6}<k^{6k^6}$$

这就是说，$t=T+1$时（2）仍然成立。把（2）代入（1）得

$$|T(n,\ m)|<k^{6k^6} \qquad (3)$$

又因为当$p_1|k,\ \cdots,p_t|k$时，从$p_1<\cdots<p_t$可推出$t<k$，从而由Ⅱ）可得

$$|T(n,\ m)| = |T(n_1,\ p_1^{a_1})|\cdots|T(n_t,\ p_t^{a_t})|$$
$$\leqslant k\cdots k=k^t<k^k. \qquad (4)$$

故从（3）、（4）再结合Ⅰ）、Ⅳ）立刻得到

$$|T(n,\ m)| = |m^{-1+v}S(n,\ m)|<k^{6k^6}\cdot k^k$$
$$=k^{6k^6+k},$$

设$c=k^{6k^{6}+k}$，并注意到$v=\frac{1}{k}$，就有

$$|S(n,\ m)|<cm^{1-\frac{1}{k}}.$$

第八章　与椭圆模函数有关的几个数论问题

一、提　　要

定义　$$q_0=\prod_{n=1}^{\infty}(1-q^{2n}),$$

$$q_1=\prod_{n=1}^{\infty}(1+q^{2n}),$$

$$q_2=\prod_{n=1}^{\infty}(1+q^{2n-1}),$$

$$q_3=\prod_{n=1}^{\infty}(1-q^{2n-1}).$$

其中q可为实数，也可为复数。显然，当$|q|<1$时，它们都是收敛的。

定理1　若$|q|<1$，则

$$q_1q_2q_3=1.$$

定义　以$p(n)$表正整数n的分拆种数，若限定分拆中每一部分不超过r，则此类分拆数以$p_r(n)$表示。

定理2　若$|q|<1$，则

$$1+\sum_{n=1}^{\infty}p_r(n)q^n=\frac{1}{(1-q)(1-q^2)\cdots(1-q^r)};$$

$$1+\sum_{n=1}^{\infty}p(n)q^n=\frac{1}{q_0q_3}.$$

定理 3　命$q(n)$表示把n分为若干个奇数的和的分拆种数，则

$$1+\sum_{n=1}^{\infty}q(n)q^n=\frac{1}{q_3}.$$

定理 4　q_1q_2展开式中q^n的系数，等于把n分为不相等部分的分拆种数。

定理 5　把n分为不等数和的分拆数，等于把n分为奇数和的分拆数。

定理 6　若$|q|<1$，$z\neq 0$，则有

$$\prod_{n=1}^{\infty}\left((1-q^{2n})(1+q^{2n-1}z)(1+q^{2n-1}z^{-1})\right)$$

$$=1+\sum_{n=1}^{\infty}q^{n^2}(z^n+z^{-n})$$

$$=\sum_{n=-\infty}^{\infty}q^{n^2}z^n.$$

定理 7　命$E(n)$代表把n分为偶数个不等数和的分拆数（偶分拆数），$U(n)$代表把n分为奇数个不等数和的分拆数（奇分拆数），则

$$E(n)-U(n)=\begin{cases}0, & 若n\neq\frac{1}{2}k(3k\pm 1)\\ (-1)^k, & 若n=\frac{1}{2}k(3k\pm 1)\end{cases}$$

定理 8　当$n>1$时，

$$2^{[\sqrt{n}]}<p(n)<n^{3[\sqrt{n}]}.$$

定理 9

$$\lim_{n\to\infty}\frac{\log p(n)}{n^{\frac{1}{2}}}=\pi\sqrt{\frac{2}{3}}.$$

定义　用$r_s(n)$表示

$$x_1^2+\cdots x_s^2=n$$

的整数解$(x_1\cdots x_s)$的组数。

定理10

$$r_2(n)=4\sum_{\substack{u\mid n\\ 2\nmid u}}(-1)^{\frac{1}{2}(u-1)}$$

$$r_4(n)=8\sum_{\substack{m\mid n\\ 4\nmid m}}m$$

定理11　$\frac{r_4(n)}{8}$是一积性函数。

定理12　任一正整数都可以表示成四个平方数的和。

定理13　命$s_4(n)$表

$$x_1(x_1+1)+x_2(x_2+1)+x_3(x_3+1)+x_4(x_4+1)+1=n$$

的解数，当n是奇数时，则

$$s_4(n)=2r_4(n).$$

定义　用$r_s(n,\ q)$表示

$$x_1^2+\cdots+x_s^2\equiv n(\bmod q)$$

的解数。

定义
$$\Delta q(n)=\frac{r(n,q)}{q^{s-1}}$$

$$\partial_p(n)=\lim_{l\to\infty}\Delta_{p^l}(n)$$

后者称为不定方程

$$x_1^2+\cdots+x_s^2\equiv n(\mathrm{mod}\,q)$$

的p密率。

定义　不定方程

$$x_1^2+\cdots+x_s^2\equiv n(\mathrm{mod}\,q)$$

的实密率用$\partial_0(n)$表示，其中$\partial_0(n)$等于

$$\partial_0(n)=\lim_{\delta\to 0}\frac{1}{2\delta}\int\cdots\cdots\cdots\cdots\cdots\cdots\int_{n-\delta\leqslant x_1^2+\cdots+x_s^2\leqslant n+\delta} dx_1\cdots dx_n.$$

定理14　当s是偶数时，实密率等于

$$\frac{\pi^{s/2}}{\left(\frac{s}{2}-1\right)!}n^{\frac{s}{2}-1}.$$

定义

$$A_{p^l}(n)=\sum_{\substack{a=1\\ p\nmid a}}^{p^l}\frac{1}{p^{sl}}\left(\sum_{x=1}^{p^l}e^{2\pi iax^2/p^l}\right)^s e^{-2\pi ian/p^l}.$$

定理15

$$\sum_{m=0}^{l}A_{p^m}(n)=\Delta_{p^l}(n).$$

定理16　若$s=4r$且p是奇素数时，则

$$A_{p^l}(n)=p^{-2rl}C_{p^l}(n).$$

定理17　若$s=4r$，则

$$A_2(n)=0.$$

定理18　设$s=4r$，$p\neq 2$，$p^\tau\|n$，则

$$\partial_p(n)=(1-p^{-2r})\sum_{l=0}^{\tau}p^{-(2r-1)l}$$

$$=(1-p^{-2r})(p^\tau)^{-(2r-1)}\sigma_{2r-1}(p^\tau).$$

定理19　设$s=4r$，$2^{\tau}\|n$，则，

$$\partial_2(n)=\begin{cases}1, & 若\tau=0,\\ (1-2^{2-2r}+2^{(1-2r)(\tau+1)}(2^{2r}-1))(1-2^{1-2r})^{-1}, & 若\tau>0,\ 2\nmid r\\ (1-2^{(1-2r)(\tau+1)}(2^{2r}-1))(1-2^{1-2r})^{-1}, & 若\tau>0,\ 2\mid r\end{cases}$$

定义　命

$$S_s(n)=\prod_p \partial_p(n),$$

及

$$\delta_s(n)=\partial_0(n)S_s(n).$$

定理20　若$s=4$，则

$$\delta_4(n)=r_4(n);$$

若$s=8$，则

$$\delta_8(n)=16(-1)^n\sum_{d\mid n}(-1)^d d^3.$$

定理21　当$3\leqslant s\leqslant 8$时，

$$r_s(n)=\delta_s(n).$$

二、题　　解

§3　Jacobi等式

习题1　求证当$|q|<1$时，

$$\prod_{n=0}^{\infty}\left((1-q^{5n+1})(1-q^{5n+4})(1-q^{5n+5})\right)$$

$$=\sum_{n=-\infty}^{\infty}(-1)^n q^{\frac{1}{2}n(5n+3)},$$

$$\prod_{n=0}^{\infty}\Big((1-q^{5n+2})(1-q^{5n+3})(1-q^{5n+5})\Big)$$

$$=\sum_{n=-\infty}^{\infty}(-1)^n q^{\frac{1}{2}n(5n+1)}.$$

证： 先证第一式。取 $q^{\frac{5}{2}}$ 代 q，$-q^{\frac{3}{2}}$ 代 z，由提要中定理6得

$$\prod_{n=1}^{\infty}\left[1-\left(q^{\frac{5}{2}}\right)^{2n}\right]\left[1+\left(q^{\frac{5}{2}}\right)^{2n-1}\left(-q^{\frac{3}{2}}\right)\right]$$

$$\left[1+\left(q^{\frac{5}{2}}\right)^{2n-1}\left(-q^{-\frac{3}{2}}\right)\right]$$

$$=\prod_{n=1}^{\infty}(1-q^{5n})(1-q^{5n-1})(1-q^{5n-4})$$

$$=\sum_{n=-\infty}^{\infty}\left(q^{\frac{5}{2}}\right)^{n^2}\left(-q^{\frac{3}{2}}\right)^{n}$$

$$=\sum_{n=-\infty}^{\infty}(-1)^n q^{\frac{1}{2}n(5n+3)}$$

再由 $\prod_{n=0}^{\infty}(1-q^{5n+1})(1-q^{5n+4})(1-q^{5n+5})$

$$=\prod_{n=1}^{\infty}(1-q^{5n})(1-q^{5n-1})(1-q^{5n-4})$$

可知第一个等式成立。以 $q^{\frac{5}{2}}$ 代 q，$-q^{\frac{1}{2}}$ 代 z 得

$$\prod_{n=1}^{\infty}\left[1-\left(q^{\frac{5}{2}}\right)^{2n}\right]\left[1+\left(q^{\frac{5}{2}}\right)^{2n-1}\left(-q^{\frac{1}{2}}\right)\right]$$
$$\left[1+\left(q^{\frac{5}{2}}\right)^{2n-1}\left(-q^{-\frac{1}{2}}\right)\right]$$

$$=\prod_{n=1}^{\infty}(1-q^{5n})(1-q^{5n-2})(1-q^{5n-3})$$

$$=\sum_{n=-\infty}^{\infty}\left(q^{\frac{5}{2}}\right)^{n^2}\left(-q^{\frac{1}{2}}\right)^{n}$$

$$=\sum_{n=-\infty}^{\infty}(-1)^n q^{\frac{1}{2}n(5n+1)}$$

又由 $\prod_{n=0}^{\infty}\left(1-q^{5n+2}\right)\left(1-q^{5n+3}\right)\left(1-q^{5n+5}\right)$

$$=\prod_{n=1}^{\infty}\left(1-q^{5n}\right)\left(1-q^{5n-2}\right)\left(1-q^{5n-3}\right)$$

可知第二个等式也成立。

习题 2 证明

$$q(1-q^{24})(1-q^{2\cdot 24})(1-q^{3\cdot 24})\cdots$$
$$=q^{1^2}-q^{5^2}-q^{7^2}+q^{11^2}+q^{13^2}-q^{17^2}-\cdots$$

$$q\Big((1-q^{8})(1-q^{2\cdot 8})(1-q^{3\cdot 8})\cdots\Big)^{3}$$
$$=q^{1^2}-3q^{3^2}+5q^{5^2}-7q^{7^2}+\cdots.$$

证： 设$g=q^{24}$，那么

$$(1-q^{24})(1-q^{2\cdot 24})(1-q^{3\cdot 24})\cdots$$

$$=\prod_{n=1}^{\infty}(1-q^{24n})$$

$$= \prod_{n=1}^{\infty}(1-g^n)$$

$$= \prod_{n=1}^{\infty}(1-g^{3n})(1-g^{3n-1})(1-g^{3n-2})$$

以$-g^{\frac{3}{2}}$代g，取$z=g^{\frac{1}{2}}$，则由提要中定理 6

$$\prod_{n=1}^{\infty}(1-g^{3n})(1-g^{3n-1})(1-g^{3n-2})$$

$$= \sum_{n=-\infty}^{\infty}\left(-g^{\frac{3}{2}}\right)^{n^2}\left(g^{\frac{1}{2}}\right)^{n}$$

$$= \sum_{n=-\infty}^{\infty}(-1)^n g^{\frac{1}{2}n(3n+1)}$$

$$= 1+\sum_{n=1}^{\infty}(-1)^n\left(g^{\frac{1}{2}n(3n-1)}+g^{\frac{1}{2}(3n+1)}\right)$$

$$= 1-g-g^2+g^5+g^7-g^{12}-g^{15}+\cdots$$

又因为$g=q^{24}$，从而

$$\prod_{n=1}^{\infty}(1-q^{24n})$$

$$= 1-q^{24}-q^{2\cdot 24}+q^{5\cdot 24}+q^{7\cdot 24}-q^{12\cdot 24}-q^{15\cdot 24}+\cdots$$

故 $$q\prod_{n=1}^{\infty}(1-q^{24n})$$

$$= q-q^{24+1}-q^{2\cdot 24+1}+q^{5\cdot 24+1}+ + q^{7\cdot 24+1}-q^{12\cdot 24+1}$$

$$-q^{15\cdot 24+1}+\cdots$$

$$= q-q^{5^2}-q^{7^2}+q^{11^2}+q^{13^2}-q^{17^2}-\cdots$$

此即第一式。设$g=q^8$，则

$$(1-q^8)(1-q^{2\cdot 8})(1-q^{3\cdot 8})\cdots$$

$$=\prod_{n=1}^{\infty}(1-q^{8n})$$

$$=\prod_{n=1}^{\infty}(1-g^{n})$$

用 $g^{\frac{1}{2}}$代g，$g^{\frac{1}{2}}\xi$代z，则又有

$$\prod_{n=1}^{\infty}(1-g^{n})(1+g^{n}\xi)(1+g^{n-1}\xi^{-1})$$

$$=\sum_{n=-\infty}^{\infty} g^{\frac{1}{2}n(n+1)}\xi^{n}$$

即$$\frac{\xi+1}{\xi}\prod_{n=1}^{\infty}(1-g^{n})(1+g^{n}\xi)(1+g^{n}\xi^{-1})$$

$$=\sum_{n=-\infty}^{\infty} q^{\frac{1}{2}n(n+1)}\xi^{n} \qquad (1)$$

显然$$\lim_{\xi\to-1}\prod_{n=1}^{\infty}(1-g^{n})(1+g^{n}\xi)(1+g^{n}\xi^{-1})$$

$$=\left(\prod_{n=1}^{\infty}(1-g^{n})\right)^{3} \qquad (2)$$

又因$$\sum_{n=-\infty}^{\infty}(-1)^{n}g^{\frac{1}{2}n(n+1)}$$

$$=\sum_{n=0}^{\infty}(-1)^{n}g^{\frac{1}{2}n(n+1)}+\sum_{n=-\infty}^{-1}(-1)^{n}g^{\frac{1}{2}n(n+1)}$$

$$=\sum_{n=0}^{\infty}(-1)^{n}g^{\frac{1}{2}n(n+1)}+\sum_{m=0}^{\infty}(-1)^{m+1}g^{\frac{1}{2}m(m+1)}=0$$

因此$\frac{\xi}{\xi+1}\sum_{n=-\infty}^{\infty} g^{\frac{1}{2}n(n+1)}\xi^n$

$$=\frac{\xi}{\xi+1}\sum_{n=-\infty}^{\infty} g^{\frac{1}{2}n(n+1)}\xi^n-\frac{\xi}{\xi+1}\sum_{n=-\infty}^{\infty}(-1)^n g^{\frac{1}{2}n(n+1)}$$

$$=\frac{\xi}{\xi+1}\sum_{n=-\infty}^{\infty} g^{\frac{1}{2}n(n+1)}(\xi^n-(-1)^n)$$

$$=\sum_{n=-\infty}^{\infty} q^{\frac{1}{2}n(n+1)}\frac{\xi(\xi^n-(-1)^n)}{\xi+1};$$

注意到 $\lim\limits_{\xi\to-1}\frac{\xi^n-(-1)^n}{\xi+1}=(-1)^{n-1}n$，从而

$$\lim_{\xi\to-1}\frac{\xi}{\xi+1}\sum_{n=-\infty}^{\infty} g^{\frac{1}{2}n(n+1)}\xi^n=\sum_{n=-\infty}^{\infty}(-1)^n ng^{\frac{1}{2}n(n+1)} \quad (3)$$

由（1）、（2）、（3）式便有

$$\left(\prod_{n=1}^{\infty}(1-g^n)\right)^3=\sum_{n=-\infty}^{\infty}(-1)^n ng^{\frac{1}{2}n(n+1)}$$

以$g=q^8$代入上式就有

$$\left(\prod_{n=1}^{\infty}(1-q^{8n})\right)^3=\sum_{n=-\infty}^{\infty}(-1)^n nq^{4n(n+1)}$$

$$=1-3q^8+5q^{3\cdot8}-7q^{6\cdot8}+\cdots$$

故 $q\left(\prod_{n=1}^{\infty}(1-q^{8n})\right)^3=q-3q^{3^2}+5q^{5^2}-7q^{7^2}+\cdots$

第二个等式由此得证。

§5 分拆之图解法

习题1 证明

$$\frac{1}{(1-q)(1-q^2)(1-q^3)\cdots}=1+\frac{q}{(1-q)^2}+$$

$$\frac{q^4}{(1-q)^2(1-q^2)^2}+\frac{q^9}{(1-q)^2(1-q^2)^2(1-q^3)^2}+\cdots$$

证：把正整数n的一分拆，按每行左边对齐并依次减少的次序排列，例如：

$$19=7+5+4+2+1,$$

```
• • • | • • • •
• • • | • •
• • • | •
-------
• •
•
```

如果设该分拆图左上角所含最大正方形的边长为t（上图$t=3$，$n=19$），注意到该正方形块下方和右方的分拆，可以得出：对任一固定的t，该图表明n的分拆数等于$n-t^2$按两种方式分成不超过t份的分拆数。具体而言，就是等于不定方程

$$x_1+2x_2+\cdots+tx_t+y_1+2y_2+\cdots+ty_t=n-t^2$$

（上图为$x_1+2x_2+3x_3+y_1+2y_2+3y_3=10$）的非负整数解数，这就是

$$\frac{q^{t^2}}{(1-q)^2(1-q^2)^2\cdots(1-q^t)^2}$$

展开式中q^n的系数，再由提要中定理2可得

$$\frac{1}{(1-q)(1-q^2)(1-q^3)\cdots}$$

$$=\sum_{t=0}^{\infty}\frac{q^{t^2}}{(1-q)^2(1-q^2)^2\cdots(1-q^t)^2}$$

此即所要求证的等式。须注意的是，$t=0$ 对应的项为 1 。

习题 2　用图表法证明定理4.4.

证：本题所要证明的定理4.4为：当$|q|<1$时，

$$(1+q)(1+q^2)(1+q^3)\cdots$$

$$=1+\frac{q}{1-q}+\frac{q^3}{(1-q)(1-q^2)}+\cdots+\frac{q^{\frac{1}{2}m(m+1)}}{(1-q)(1-q^2)\cdots(1-q^m)}$$

$$+\cdots$$

把正整数n分成不等部分的一分拆，每行从左边开始缩一格排列，例如：

$$19=7+5+4+2+1$$

```
• • • • •|• •
  • • • •|•
    • • •|•
      • •|
        •|
```

设竖线左边所含最大等腰直角三角形的腰长为t（上图$t=5$，$n=19$），再注意到竖线右边的分拆，可以得出：对任一固定的t，该图所示把n分成不等部分和的分拆数为

$$n-(1+2+\cdots+t)=n-\frac{t(t+1)}{2}$$

不超过t份的分拆数，这就是

$$\frac{q^{\frac{1}{2}t(t+1)}}{(1-q)(1-q^2)\cdots(1-q^t)}$$

展开式中q^n的系数。再由提要中定理 4 立得

$$(1+q)(1+q^2)(1+q^3)\cdots$$

$$=\sum_{t=0}^{\infty}\frac{q^{\frac{1}{2}t(t+1)}}{(1-q)(1-q^2)\cdots(1-q^t)}$$

此即所要求证的等式。须注意的是，$t=0$ 对应的项为 1。

§7 平方和问题

习题 1 经由以下之办法算出

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots=\frac{\pi^2}{6}.$$

由四维空间球

$$u^2+v^2+w^2+z^2\leqslant x$$

中之整点数$A(x)$之渐近公式

$$A(x)=\frac{\pi^2}{2}x^2+O\left(x^{\frac{3}{2}}\right),$$

并用定理 2 以求出另一表法。比较之而得习题中所求。

证：由定理 2（即提要中定理10），四维空间球

$$u^2+v^2+w^2+z^2\leqslant x$$

内的整点数$A(x)$可写成

$$A(x)=\sum_{n\leqslant x}r_4(n)=\sum_{n\leqslant x}8\sum_{\substack{m|n\\4\nmid m}}m$$

$$=\sum_{n\leqslant x}8\left(\sum_{m|n}m-\sum_{4m|n}4m\right)=8\sum_{n\leqslant x}\sum_{m|n}m-32\sum_{n\leqslant x}\sum_{4m|n}m$$

$$=8\sum_{dd'\leqslant x}d'-32\sum_{d_1d_1'\leqslant\frac{x}{4}}d_1'$$

设
$$1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots=\delta$$

那么

$$\sum_{dd'\leqslant x}d'=\sum_{d=1}^{[x]}\sum_{d'=1}^{[x/d]}d'=\sum_{d=1}^{[x]}\frac{1}{2}\left[\frac{x}{d}\right]\left(\left[\frac{x}{d}\right]+1\right)$$

$$=\frac{1}{2}\sum_{d=1}^{[x]}\left(\left[\frac{x}{d}\right]^{2}+\left[\frac{x}{d}\right]\right)$$

$$=\frac{1}{2}\sum_{d=1}^{[x]}\left(\frac{x^{2}}{d^{2}}+O\left(\frac{x}{d}\right)\right)$$

$$=\frac{1}{2}x^{2}\sum_{d=1}^{[x]}\frac{1}{d^{2}}+O\left(x\sum_{d=1}^{[x]}\frac{1}{d}\right)$$

$$=\frac{1}{2}x^{2}\sum_{d=y}^{\infty}\frac{1}{d^{2}}+O\left(x^{2}\sum_{d>[x]}^{\infty}\frac{1}{d^{2}}\right)+O(x\log x)$$

$$=\frac{1}{2}\delta x^{2}+O(x\log x) \qquad (1)$$

同理 $$\sum_{d_1 d_1'\leqslant\frac{x}{4}} d_1'=\frac{1}{32}\delta x^{2}+O(x\log x) \qquad (2)$$

从而 $$A(x)=8\sum_{dd'\leqslant x} d'-32\sum_{d_1 d_1'\leqslant\frac{x}{4}} d_1'$$

$$=8\cdot\frac{1}{2}\delta x^{2}-32\cdot\frac{1}{32}\delta x^{2}+O(x\log x)$$

$$=3\delta x^{2}+O(x\log x) \qquad (3)$$

又由题设 $$A(x)=\frac{\pi^{2}}{2}x^{2}+O\left(x^{\frac{8}{2}}\right)$$

从而 $$A(x)\sim\frac{\pi^{2}}{2}x^{2}$$

结合（3）可得 $$3\delta x^{2}\sim\frac{\pi^{2}}{2}x^{2}$$

故 $$3\delta=\frac{\pi^{2}}{2}$$

$$\delta=\frac{\pi^2}{6}$$

此即 $$1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots=\frac{\pi^2}{6}$$

把 $\delta=\frac{\pi^2}{6}$代入（3），就能得到较

$$A(x)=\frac{\pi^2}{2}x^2+O\left(x^{\frac{3}{2}}\right)$$

更精密一些的结果：

$$A(x)=\frac{\pi^2}{2}x^2+O(x\log x)\ .$$

习题 2 算出

$$\left(\frac{1}{6}+\frac{x}{1-x}-\frac{x^2}{1-x^2}+\frac{x^4}{1-x^4}-\frac{x^5}{1-x^5}+\cdots\right)^2$$

$$=\frac{1}{36}+\frac{1}{3}\left(\frac{x}{1-x}+\frac{2x^2}{1-x^2}+\frac{4x^4}{1-x^4}+\frac{5x^5}{1-x^5}+\cdots\right)$$

证：设 $$u_r=\frac{x^r}{1-x^r}$$

则上式可写成

$$\left(\frac{1}{6}+\sum_{n=0}^{\infty}u_{3n+1}-\sum_{n=0}^{\infty}u_{3n+2}\right)^2=\frac{1}{36}+\frac{1}{3}\sum_{\substack{n=1\\3\nmid n}}^{\infty}nu_n \qquad (1)$$

从定理 5 知，当θ是一实数而非π的偶数倍时

$$\left(\frac{1}{6}\text{ctg}\tfrac{1}{2}\theta+u_1\sin\theta+u_2\sin2\theta+\cdots\right)^2$$

$$=\left(\frac{1}{4}\text{ctg}\tfrac{1}{2}\theta\right)^2+C_0+\sum_{k=1}^{\infty}C_k\cos k\theta \qquad (2)$$

此处 $C_0=\frac{1}{2}\sum_{n=1}^{\infty}nu_n$

$$C_k=u_k\left(1+u_k-\frac{1}{2}k\right),\quad k\geqslant 1$$

在（2）式中令$\theta=\frac{2\pi}{3}$，由$\sin 3n\cdot\frac{2\pi}{3}=0$，$\sin(3n+1)\frac{2\pi}{3}=\frac{\sqrt{3}}{2}$，$\sin(3n+2)\frac{2\pi}{3}=-\frac{\sqrt{3}}{2}$，$\cos 3n\cdot\frac{2\pi}{3}=1$，$\cos(3n\pm 1)\frac{2\pi}{3}=-\frac{1}{2}$ 可得

$$\left(\frac{1}{6}+\sum_{n=0}^{\infty}u_{3n+1}-\sum_{n=0}^{\infty}u_{3n+2}\right)^2$$

$$=\frac{1}{36}+\frac{2}{3}\sum_{n=1}^{\infty}nu_n+\frac{4}{3}\sum_{n=1}^{\infty}C_{3n}-\frac{2}{3}\sum_{\substack{n=1\\3\nmid n}}^{\infty}C_n$$

$$=\frac{1}{36}+\frac{2}{3}\sum_{n=1}^{\infty}nu_n+\frac{4}{3}\sum_{n=1}^{\infty}u_{3n}\left(1+u_{3n}-\frac{3}{2}n\right)$$

$$-\frac{2}{3}\sum_{\substack{n=1\\3\nmid n}}^{\infty}u_n\left(1+u_n-\frac{1}{2}n\right)$$

$$=\frac{1}{36}+\frac{2}{3}\sum_{n=1}^{\infty}nu_n+\frac{4}{3}\sum_{n=1}^{\infty}u_{3n}(1+u_{3n})-2\sum_{n=1}^{\infty}nu_{3n}$$

$$-\frac{2}{3}\sum_{\substack{n=1\\3\nmid n}}^{\infty}u_n(1+u_n)+\frac{1}{3}\sum_{\substack{n=1\\3\nmid n}}^{\infty}nu_n. \qquad (3)$$

由于 $\sum_{n=1}^{\infty} u_n(1+u_n)=\sum_{n=1}^{\infty}\frac{x^n}{1-x^n}\left(1+\frac{x^n}{1-x^n}\right)$

$$=\sum_{n=1}^{\infty}\frac{x^n}{(1-x^n)^2}=\sum_{n=1}^{\infty}\sum_{m=1}^{\infty} m x^{nm}=\sum_{m=1}^{\infty} m\sum_{n=1}^{\infty} x^{mn}$$

$$=\sum_{m=1}^{\infty} m\frac{x^m}{1-x^m}=\sum_{m=1}^{\infty} m u_m=\sum_{n=1}^{\infty} n u_n$$

同理 $\sum_{n=1}^{\infty} u_{3n}(1+u_{3n})=\sum_{n=1}^{\infty} n u_{3n}$

因此 $\frac{4}{3}\sum_{n=1}^{\infty} u_{3n}(1+u_{3n})-2\sum_{n=1}^{\infty} n u_{3n}-\frac{2}{3}\sum_{\substack{n=1\\3\nmid n}}^{\infty} u_n(1+u_n)$

$$=\frac{4}{3}\sum_{n=1}^{\infty} u_{3n}(1+u_{3n})-2\sum_{n=1}^{\infty} u_{3n}(1+u_{3n})$$

$$-\frac{2}{3}\sum_{\substack{n=1\\3\nmid n}}^{\infty} u_n(1+u_n)$$

$$=-\frac{2}{3}\sum_{n=1}^{\infty} u_{3n}(1+u_{3n})-\frac{2}{3}\sum_{\substack{n=1\\3\nmid n}}^{\infty} u_n(1+u_n)$$

$$=-\frac{2}{3}\sum_{n=1}^{\infty} u_n(1+u_n)=-\frac{2}{3}\sum_{n=1}^{\infty} n u_n \qquad (4)$$

把（4）代入（3）立得（1），即本题结论成立。

又：如果设

$$\frac{x}{1-x}+\frac{2x^2}{1-x^2}+\frac{4x^4}{1-x^2}+\frac{5x^2}{1-x^5}+\cdots=\sum_{n=1}^{\infty} r(n)x^n$$

$$\frac{x}{1-x}-\frac{1-x^2}{1-x^2}+\frac{x^4}{1-x^4}+\frac{x^5}{1-x^5}+\cdots=\sum_{n=1}^{\infty}r_1(n)x^n$$

则原题等式变成：

$$\frac{1}{36}+\frac{1}{3}x+\frac{1}{3}\sum_{n=2}^{\infty}\left(r_1(n)+3\sum_{t=1}^{n-1}r_1(n-t)r_1(t)\right)x^n$$

$$=\frac{1}{36}+\frac{1}{3}x+\frac{1}{3}\sum_{n=2}^{\infty}r(n)x^n \qquad (5)$$

容易知道，此处$r(n)$是n的形如$3k+1$的因子与形如$3k+2$的因子的总和，$r_1(n)$是n的形如$3k+1$的因子数与形如$3k+2$的因子数之差。形式幂级数的用途很多，比如我们可以用它来确定一次不定方程整数解的个数（第一章第八节习题3）。通过本题，还知道可以利用它来证明一些关于数论函数的恒等式，而证法比较简单和明了，例如从（5）式立刻得到

$$r(n)=r_1(n)+3\sum_{t=1}^{n-1}r_1(n-t)r_1(t),\quad n\geqslant 2$$

特殊地，当$n=3^k$时，由于$r(n)=r_1(n)=1$。
得

$$\sum_{t=1}^{n-1}r_1(n-t)r_1(t)=0,\quad n\geqslant 2.$$

习题3 利用

$$(1-\cos n\theta)\operatorname{ctg}^2\tfrac{1}{2}\theta=(2n-1)+4(n-1)\cos\theta$$
$$+4(n-2)\cos 2\theta+\cdots+4\cos(n-1)\theta+\cos n\theta$$

以证明

$$\left\{\frac{1}{8}\operatorname{ctg}^2\tfrac{1}{2}\theta+\frac{1}{12}+\frac{x}{1-x}(1-\cos\theta)+\frac{2x^2}{1-x^2}(1-\cos 2\theta)\right.$$
$$\left.+\frac{3x^3}{1-x^3}(1-\cos 3\theta)+\cdots\right\}^2=\left(\frac{1}{8}\operatorname{ctg}^2\tfrac{1}{2}\theta+\frac{1}{12}\right)^2+$$

$$+\frac{1}{12}\left\{\frac{1^3x}{1-x}(5+\cos\theta)+\frac{2^3x^2}{1-x^2}(5+\cos2\theta)\right.$$

$$\left.+\frac{3^3x^3}{1-x^3}(5+\cos3\theta)+\cdots\right\}.$$

证： 令$u_l=\dfrac{x^l}{1-x^l}$，则上式变成

$$\left\{\frac{1}{8}\text{ctg}^2\tfrac{1}{2}\theta+\frac{1}{12}+\sum_{n=1}^{\infty}nu_n(1-\cos n\theta)\right\}^2$$

$$=\left(\frac{1}{8}\text{ctg}^2\tfrac{1}{2}\theta+\frac{1}{12}\right)^2+\frac{1}{12}\sum_{n=1}^{\infty}n^3u_n(5+\cos n\theta) \qquad (1)$$

因为

$$\left\{\frac{1}{8}\text{ctg}^2\tfrac{1}{2}\theta+\frac{1}{12}+\sum_{n=1}^{\infty}nu_n(1-\cos n\theta)\right\}^2$$

$$=\left(\frac{1}{8}\text{ctg}^2\tfrac{1}{2}\theta+\frac{1}{12}\right)^2+\frac{1}{4}\sum_{n=1}^{\infty}\text{ctg}^2\tfrac{1}{2}\theta\cdot nu_n(1-\cos n\theta)$$

$$+\frac{1}{6}\sum_{n=1}^{\infty}nu_n(1-\cos n\theta)+\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}mnu_m u_n(1-\cos m\theta)(1-\cos n\theta)$$

并且 $\dfrac{1}{4}\displaystyle\sum_{n=1}^{\infty}nu_n(1-\cos n\theta)\text{ctg}^2\tfrac{1}{2}\theta$

$$=\frac{1}{4}\sum_{n=1}^{\infty}nu_n\Big((2n-1)+4(n-1)\cos\theta+4(n-2)\cos2\theta$$

$$+\cdots+4\cos(n-1)\theta+\cos n\theta\Big);$$

$$\frac{1}{6}\sum_{n=1}^{\infty}nu_n(1-\cos n\theta)=\frac{1}{6}\sum_{n=1}^{\infty}nu_n-\frac{1}{6}\sum_{n=1}^{\infty}nu_n\cos n\theta;$$

$$\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} mnu_m u_n(1-\cos m\theta)(1-\cos n\theta)$$

$$=\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} mnu_m u_n-\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} mnu_m u_n(\cos m\theta+\cos n\theta)+$$

$$+\frac{1}{2}\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} mnu_m u_n\Big(\cos(m-n)\theta+\cos(m+n)\theta\Big)$$

所以 $\left\{\frac{1}{8}\mathrm{ctg}^2\frac{1}{2}\theta+\frac{1}{12}+\sum_{n=1}^{\infty} nu_n(1-\cos n\theta)\right\}^2$

$$=\left(\frac{1}{8}\mathrm{ctg}^2\frac{1}{2}\theta+\frac{1}{12}\right)^2+\frac{1}{4}\sum_{n=1}^{\infty}(2n-1)nu_n$$

$$+\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} mnu_m u_n+\frac{1}{2}\sum_{n=1}^{\infty} n^2 u_n{}^2+\frac{1}{6}\sum_{n=1}^{\infty} nu_n+\sum_{k=1}^{\infty} C_k\cos k\theta$$

$$=\left(\frac{1}{8}\mathrm{ctg}^2\frac{1}{2}\theta+\frac{1}{12}\right)^2-\frac{1}{12}\sum_{n=1}^{\infty} nu_n+\frac{1}{2}\sum_{n=1}^{\infty} n^2 u_n$$

$$+\sum_{m=1}^{\infty}\sum_{n=1}^{\infty} mnu_m u_n+\frac{1}{2}\sum_{n=1}^{\infty} n^2 u_n{}^2+\sum_{k=1}^{\infty} C_k\cos k\theta$$

其中 $C_k=\frac{1}{4}ku_k+\frac{1}{4}\sum_{l=1}^{\infty}4\ (k+l)lu_{k+l}-2\sum_{n=1}^{\infty} ku_k nu_n$

$$-\frac{1}{6}ku_k+\sum_{\substack{m=1\\m-n=k}}^{\infty}\sum_{n=1}^{\infty} mnu_m u_n+\frac{1}{2}\sum_{\substack{m=1\\m+n=k}}^{\infty}\sum_{n=1}^{\infty} mnu_m u_n$$

$$=\frac{1}{12}ku_k+\sum_{l=1}^{\infty}(k+l)lu_{k+l}-2ku_k\sum_{n=1}^{\infty} nu_n+$$

$$+\sum_{l=1}^{\infty}(k+l)lu_{k+l}u_l+\frac{1}{2}\sum_{l=1}^{k-1}l(k-l)u_lu_{k-l}.$$

另一方面

$$\frac{1}{12}\sum_{n=1}^{\infty}n^3u_n(5+\cos n\theta)$$

$$=\frac{5}{12}\sum_{n=1}^{\infty}n^3u_n+\frac{1}{12}\sum_{n=1}^{\infty}n^3u_n\cos n\theta$$

所以（1）式成立的充要条件是

$$\frac{5}{12}\sum_{n=1}^{\infty}n^3u_n=-\frac{1}{12}\sum_{n=1}^{\infty}nu_n+\frac{1}{2}\sum_{n=1}^{\infty}n^2u_n$$

$$+\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}mnmu_{\ }+\frac{1}{2}\sum_{n=1}^{\infty}n^2u_n{}^2 \qquad (2)$$

且 $$\frac{1}{12}k^3u_{\ }=\frac{1}{12}ku_k+\sum_{l=1}^{\infty}(k+l)lu_{k+l}-2ku_k\sum_{n=1}^{\infty}nu_n$$

$$+\sum_{l=1}^{\infty}(k+l)lu_{k+l}u_l+\frac{1}{2}\sum_{l=1}^{k-1}l(k-l)u_lu_{k-l} \qquad (3)$$

下面只证（3）式，用类似的方法可证（2）式。

因为 $u_{k+l}+u_lu_{k+l}=u_k(u_l-u_{k+l})$

$$u_lu_{k-l}=u_k(1+u_l+u_{k-l})$$

所以（3）式右端为：

$$u_k\Big(\frac{1}{12}k+\sum_{l=1}^{\infty}(k+l)l(u_l-u_{k+l})-2k\sum_{n=1}^{\infty}nu_n$$

$$+\frac{1}{2}\sum_{l=1}^{k-1}l(k-l)(1+u_l+u_{k-l})\Big)$$

$$
\begin{aligned}
&= u_k\Big(\frac{1}{12}k + k\sum_{l=1}^{\infty} l u_l - k\sum_{l=1}^{\infty}(k+l)u_{k+l} + k^2\sum_{l=1}^{\infty}u_{k+l} \\
&+ \sum_{l=1}^{\infty} l^2 u_l - \sum_{l=1}^{\infty} l^2 u_{k+l} - 2k\sum_{n=1}^{\infty} n u_n + \frac{1}{2}k\sum_{l=1}^{k-1} l \\
&+ \frac{1}{2}k\sum_{l=1}^{k-1} l u_l + \frac{1}{2}k\sum_{l=1}^{k-1} l u_{k-l} - \frac{1}{2}\sum_{l=1}^{k-1} l^2 \\
&- \frac{1}{2}\sum_{l=1}^{k-1} l^2 u_l - \frac{1}{2}\sum_{l=1}^{k-1} l^2 u_{k-l}\Big) \\
&= (A+B)u_k
\end{aligned}
$$

其中 $$
\begin{aligned}
A &= \frac{1}{12}k + k\sum_{l=1}^{\infty} l u_l - k\sum_{l=1}^{\infty}(k+l)u_{k+l} \\
&+ k^2\sum_{l=1}^{\infty}u_{k+l} + \sum_{l=1}^{\infty} l^2 u_l - \sum_{l=1}^{\infty} l^2 u_{k+l} - 2k\sum_{n=1}^{\infty} n u_n ;
\end{aligned}
$$

$$
\begin{aligned}
B &= \frac{1}{2}k\sum_{l=1}^{k-1} l = \frac{1}{2}k\sum_{n=1}^{k-1} l u_l + \frac{1}{2}k\sum_{l=1}^{k-1} l u_{k-l} \\
&- \frac{1}{2}\sum_{l=1}^{k-1} l^2 - \frac{1}{2}\sum_{l=1}^{k-1} l^2 u_l - \frac{1}{2}\sum_{l=1}^{k-1} l^2 u_{k-l} .
\end{aligned}
$$

因为 $$
\begin{aligned}
&\sum_{l=1}^{\infty} l^2 u_l - \sum_{l=1}^{\infty} l^2 u_{k+l} \\
&= \sum_{l=1}^{\infty} l^2 u_l - \sum_{l=1}^{\infty}(k+l)^2 u_{k+l} + 2k\sum_{l=1}^{\infty} l u_{k+l} + k^2\sum_{l=1}^{\infty}u_{k+l} \\
&= \sum_{l=1}^{k} n^2 u_n + 2k\sum_{l=1}^{\infty} l u_{k+l} + k^2\sum_{l=1}^{\infty}u_{k+l}
\end{aligned}
$$

和 $\sum_{n=1}^{k} nn = \sum_{l=1}^{\infty} l u_l - \sum_{l=1}^{\infty} (k+l) u_{k+l}$

所以 $A = \frac{1}{12}k + k\sum_{n=1}^{k} nu_n + 2k^2 \sum_{l=1}^{\infty} u_{k+l} + \sum_{n=1}^{k} n^2 u_n$

$+ 2k \sum_{l=1}^{\infty} l u_{k+l} - 2k \sum_{n=1}^{\infty} nu_n$

$= \frac{1}{12}k + 2k^2 \sum_{l=1}^{\infty} u_{k+l} + 2k\sum_{l=1}^{\infty} l u_{k+l} - 2k\sum_{n=1}^{\infty} nu_n$

$+ k\sum_{n=1}^{k} nu_n + \sum_{n=1}^{k} n^2 u_n$

$= \frac{1}{12}k + 2k^2 \sum_{l=1}^{\infty} u_{k+l} + 2k\sum_{l=1}^{\infty} (k+l) u_{k+l} - 2k^2 \sum_{l=1}^{\infty} u_{k+l}$

$- 2k\sum_{n=1}^{\infty} nu_n + k\sum_{n=1}^{k} nu_n + \sum_{n=1}^{k} n^2 u_n$

$= \frac{1}{12}k + 2k\sum_{l=1}^{\infty} (k+l) u_{k+l} - 2k\sum_{n=1}^{\infty} nu_n + k\sum_{n=1}^{k} nu_n$

$+ \sum_{n=1}^{k} n^2 u_n$

$= \frac{1}{12}k + 2k\sum_{l=1}^{\infty} l u_l - 2k\sum_{l=1}^{k} l u_l - 2k\sum_{n=1}^{\infty} nu_n$

$+ k\sum_{n=1}^{k} nu_n + \sum_{n=1}^{k} n^2 u_n$

$= \frac{1}{12}k - k\sum_{l=1}^{k} l u_l + \sum_{n=1}^{k} n^2 u_n$

此即 $A=\frac{1}{12}k-k\sum_{l=1}^{k}lu_l+\sum_{n=1}^{k}n^2u_n$

又因为 $\frac{1}{2}k\sum_{l=1}^{k-1}l=\frac{1}{4}(k^3-k^2)$

$$\frac{1}{2}k\sum_{l=1}^{k-1}l^2=\frac{1}{12}(2k^3-3k^2+k)$$

和 $\sum_{l=1}^{k-1}lu_l+\sum_{l=1}^{k-1}lu_{k-l}$

$$=\sum_{l=1}^{k-1}lu_l+\sum_{l=1}^{k-1}(k-l)u_{k-l}+2\sum_{l=1}^{k-1}lu_{k-l}-k\sum_{l=1}^{k-1}u_{k-l}$$

$$=2\sum_{l=1}^{k-1}lu_l+2\sum_{l=1}^{k-1}lu_{k-l}-k\sum_{l=1}^{k-1}u_{k-l}$$

(上式用到了$\sum_{l=1}^{k-1}lu_l=\sum_{l=1}^{k-1}(k-l)u_{k-l}$)

且 $\sum_{l=1}^{k-1}l^2u_l+\sum_{l=1}^{k-1}l^2u_{k-l}$

$$=\sum_{l=1}^{k-1}k^2u_l+\sum_{l=1}^{k-1}(k-l)^2u_{k-l}+2k\sum_{l=1}^{k-1}lu_{k-l}-k^2\sum_{l=1}^{k-1}u_{k-l}$$

$$=2\sum_{l=1}^{k-1}l^2u_l+2k\sum_{l=1}^{k-1}lu_{k-l}-k^2\sum_{l=1}^{k-1}u_{k-l},$$

(上式用到了$\sum_{l=1}^{k-1}l^2u_l=\sum_{l=1}^{k-1}(k-l)^2u_{k-l}$)

所以 $B=\frac{1}{4}(k^3-k^2)-\frac{1}{12}(2k^3-3k^2+k)+k\sum_{l=1}^{k-1}lu_l$

$$+k\sum_{l=1}^{k-1} lu_{k-l}-\frac{1}{2}k^2\sum_{l=1}^{k-1}u_{k-l}-\sum_{l=1}^{k-1} l^2u_l$$

$$-k\sum_{l=1}^{k-1} lu_{k-l}+\frac{1}{2}k^2\sum_{l=1}^{k-1}u_{k-l}$$

$$=\frac{1}{12}k^3-\frac{1}{12}k+k\sum_{l=1}^{k-1}lu_l-\sum_{l=1}^{k-1}l^2u_l,$$

此即 $B=\frac{1}{12}k^3-\frac{1}{12}k+k\sum_{l=1}^{k-1}lu_l-\sum_{l=1}^{k-1}l^2u_l$

故 $A+B=\left(\frac{1}{12}k-k\sum_{l=1}^{k}lu_l+\sum_{n=1}^{k}n^2u_n\right)$

$$+\left(\frac{1}{12}k^3-\frac{1}{12}k+k\sum_{l=1}^{k-1}lu_l-\sum_{l=1}^{n-1}l^2u_l\right)$$

$$=\frac{1}{12}k^3-k\sum_{l=1}^{k-1}lu_l-k^2u_k+\sum_{n=1}^{k}n^2u_n+k\sum_{l=1}^{k-1}lu_l-\sum_{l=1}^{k-1}l^2u_l$$

$$=\frac{1}{12}k^3+\sum_{n=1}^{k-1}n^2u_n-\sum_{l=1}^{k-1}l^2u_l=\frac{1}{12}k^3.$$

从而（3）式右端等于

$$(A+B)u_k=\frac{1}{12}k^3u_k$$

这就证明了（3）式。

又 比较（2）式两端x^n的系数可得

$$5\sigma_3(n)=(6n-1)\sigma(n)+12\sum_{t=1}^{n-1}\sigma(n-t)\sigma(t)$$

其中

$$\sigma_3(n) = \sum_{d \mid n} d^3, \ \sigma(n) = \sum_{d \mid n} d.$$

而利用形式幂级数的相等，还可以得到一系列关于数论函数 $\sigma_\lambda(n)$ 的恒等式，例如：

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{t=1}^{n-1} \sigma_3(n-t)\sigma(t)$$

$$11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040 \sum_{t=1}^{n-1} \sigma_5(n-t)\sigma_3(t)$$

以上二式，请参阅《*Modular Functions and Dirichlet Series in Number Theory*》一书中第六章的练习。

§8 密率

习题 1 命 $s = 2r$。若 r 是偶数，则

$$(1-2^{-r})\zeta(r)S_s(2^\tau n')$$

$$= \begin{cases} n'^{1-r}\sigma_{r-1}(n'), \\ (1-2^{2-r}+2^{(1-r)(\tau+1)}(2^r-1))(1-2^{1-r})^{-1}n'^{1-r} \\ (1-2^{(1-r)(\tau+1)}(2^r-1)(1-2^{1-r})^{-1}n'^{1-r}\sigma_{r-1}(n'), \end{cases}$$

$$\text{若}\tau = 0$$

$$\sigma_{r-1}(n'),\ \text{若}\tau > 0,\ 2 \| r$$

$$\text{若}\tau > 0,\ 4 \mid r$$

若 r 是奇数，则

$$L(r)S_s(2^\tau n') = \left(\left(\frac{-1}{n'}\right) + \left(\frac{-1}{r}\right)2^{(1-r)(\tau+1)}\right)$$

$$= n'^{1-r}\rho_{r-1}(n')$$

此处 $L(r) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^r}$

而$\chi(n)=0,1,0,-1$，当$n\equiv 0,1,2,3 \pmod 4$ 时。

又

$$\rho_t(n)=\sum_{q\mid n}\left(\frac{-1}{q}\right)q^t .$$

证： 设$n=2^{\tau}n'$，$2\nmid n'$。

（一）$s=2r$且r为偶数时：

1）若$\tau=0$。设$r=2r_1$，$s=2r=4r_1$，$p>2$且$p^{\tau_1}\| n$。由提要中定理18

$$\partial_p(n)=(1-p^{-2r_1})(p^{\tau_1})^{-(2r_1-1)}\sigma_{2r_1-1}(p^{\tau_1})$$

和 $$\frac{1}{\zeta(s)}=\prod_p(1-p^{-s})$$

有 $$\prod_{p>2}\partial_p(n)=\frac{n'^{1-2r_1}}{(1-2^{-2r_1})\zeta(2r_1)}\sigma_{2r_1-1}(n')$$

此即 $$\prod_{p>2}\partial_p(n)=\frac{n'^{1-r}}{(1-2^{-r})\zeta(r)}\sigma_{r-1}(n')$$

又由提要中定理19 $\partial_2(n)=1$

所以 $$(1-2^{-r})\zeta(r)\prod_p\partial_p(n)=n'^{1-r}\sigma_{r-1}(n')$$

$$(1-2^{-r})\zeta(r)S_s(n')=n'^{1-r}\sigma_{r-1}(n')$$

2）若$\tau>0$，$2\| r$。设$r=2r_1$，$2\nmid r_1$，$s=2r=4r_1$。

由提要中定理18

$$\prod_{p>2}\partial_p(n)=\frac{n'^{1-2r_1}}{(1-2^{-2r_1})\zeta(2r_1)}\sigma_{2r_1-1}(n')$$

由提要中定理19

$$\partial_2(n)=(1-2^{2-2r_1}+2^{(1-2r_1)(\tau+1)}(2^{2r_1}-1))(1-2^{1-2r_1})^{-1}$$

因此 $$(1-2^{-r})\zeta(r)\prod_p\partial_p(n)$$

$$=(1-2^{2-r}+2^{(1-r)(\tau+1)}(2^r-1))(1-2^{1-r})^{-1}$$
$$n'^{1-r}\sigma_{r-1}(n')$$

此即 $(1-2^{-r})\zeta(r)S_s(2^\tau n')$
$$=(1-2^{2-r}+2^{(1-r)(\tau+1)}(2^r-1))(1-2^{1-r})^{-1}$$
$$n'^{1-r}\sigma_{r-1}(n').$$

3）若$\tau>0$且$4|r$。设$r=2r_1$，$s=2r=4r_1$，$2|r_1$，$p>2$，$p^{\tau_1}\|n$。由提要中定理18

$$\prod_{p>2}\partial_p(n)=\frac{n'^{1-2r_1}}{(1-2^{-2r_1})\zeta(2r_1)}\sigma_{2r_1-1}(n')$$

由提要中定理19

$$\partial_2(n)=(1-2^{(1-2r_1)(\tau+1)}(2^{2r_1}-1))(1-2^{1-2r_1})^{-1}$$

所以 $(1-2^{-r})\zeta(r)S_s(2^\tau n')$
$$=(1-2^{(1-r)(\tau+1)}(2^r-1))(1-2^{1-r})^{-1}n'^{1-r}\sigma_{r-1}(n').$$

（二）若$s=2r$且r为奇数时：先证明四个引理。

引理1 设$C_q(n)=\sum\limits_{(a,q)=1}e^{2\pi ian/q}$，$a$过$q$的一缩系．如果$s=2r$，$2\nmid r$，则

$$A_2(n)=0;$$
$$A_{2^m}(n)=2^{-(m-1)r}C_{2^m}(2^{m-2r}-n),\ m\geq 2.$$

由第7章第5节定理3可得

$$A_2(n)=0;$$

由第7章第5节定理7，当$2\nmid a$时有

$$\sum_{x=1}^{2^m}e^{2\pi iax^2/2^m}=\begin{cases}(1+i^a)2^{\frac{m}{2}}, & 若2|m\\ 2^{\frac{m+1}{2}}e^{\frac{\pi i}{4}a}, & 若2\nmid m且m>1\end{cases}$$

1）当m是偶数时：

$$A_{2^m}(n) = \sum_{\substack{a=1\\2\nmid a}}^{2^m} \frac{1}{2^{sm}}\left(\sum_{x=1}^{2^m} e^{2\pi i a x^2/2^m}\right)^s e^{-2\pi i a n/2^m}$$

$$= \sum_{\substack{a=1\\2\nmid a}}^{2^m} \frac{1}{2^{2rm}}\left((1+i^a)2^{\frac{m}{2}}\right)^{2r} e^{-2\pi i a n/2^m}$$

$$= \sum_{\substack{a=1\\2\nmid a}}^{2^m} \frac{1}{2^{rm}}(1+2i^a+i^{2a})^r e^{-2\pi i a n/2^m}$$

$$= \frac{1}{2^{(m-1)r}}\sum_{\substack{a=1\\2\nmid a}}^{2^m} i^{ar} e^{-2\pi i a n/2^m}$$

$$= \frac{1}{2^{(m-1)r}}\sum_{\substack{a=1\\2\nmid a}}^{2^m}\left(e^{\frac{\pi}{2}i}\right)^{ar} e^{-2\pi i a n/2^m}$$

$$= \frac{1}{2^{(m-1)r}}\sum_{\substack{a=1\\2\nmid a}}^{2^m} e^{2\pi a(2^{m-2}r-n)i/2^m}$$

$$= \frac{1}{2^{(m-1)r}} C_{2^m}(2^{m-2}r-n).$$

2）当m是奇数且$m>1$时：

$$= A_{2^m}(n) = \sum_{\substack{a=1\\2\nmid a}}^{2^m} \frac{1}{2^{2rm}}\left(2^{\frac{m+1}{2}} e^{\frac{\pi i}{4}a}\right)^{2r} e^{-2\pi i a n/2^m}$$

$$= \frac{1}{2^{(m-1)r}} \sum_{\substack{a=1 \\ 2\nmid a}}^{2^m} \left(e^{\frac{\pi}{2}i}\right)^{ar} e^{-2\pi ian/2^m}$$

$$= \frac{1}{2^{(m-1)r}} \sum_{\substack{a=1 \\ 2\nmid a}}^{2^m} e^{2\pi ia(2^{m-2}r-n)/2^m}$$

$$= \frac{1}{2^{(m-1)r}} C_{2^m}(2^{m-2}r-n) .$$

由1）、2）即知，当$m \geqslant 2$时，

$$A_{2^m}(n) = 2^{-(-1)r} C_{2^m}(2^{m-2}r-n).$$

引理2　设$n = 2^\tau n'$，$2 \nmid n'$，如果$s = 2r$且$2 \nmid r$，则

$$\partial_2(n) = \begin{cases} 1 - 2^{(1-r)(\tau+1)}, & 若 2 \| r-n' \\ 1 + 2^{(1-r)(\tau+1)}, & 若 4 \mid r-n' \end{cases}$$

第7章第4节定理4给出

$$C_{2^m}(2^{m-2}r-n) = \begin{cases} 2^m - 2^{m-1}, & 若 2^m \mid 2^{m-2}r-n \\ -2^{m-1}, & 若 2^{m-1} \| 2^{m-2}r-n \\ 0 & 若 2^{m-1} \nmid 2^{m-2}r-n \end{cases}$$

又因为当$m > 2$且$m \neq \tau + 2$时，$2^{m-1} \nmid 2^{m-2}r-n$，

从而

$$C_{2^m}(2^{m-2}r-n) = 0 ,$$

故由引理1有：

i) 当$\tau = 0$时，

$$\partial_2(n) = 1 + \sum_{m=2}^{\infty} A_{2^m}(n)$$

$$= 1 + \sum_{m=2}^{\infty} 2^{-(m-1)r} C_{2^m}(2^{m-2}r-n)$$

$$= 1 + 2^{-(2-1)r} C_{2^2}(2^{2-2}r - n')$$

$$= 1 + 2^{-r} C_{2^2}(r - n');$$

因为 $C_{2^2}(r-n') = \begin{cases} -2, & 2 \| r-n' \\ 2, & 4 \mid r-n' \end{cases}$

故 $\partial_2(n) = \begin{cases} 1 - 2^{1-r}, & 若 2 \| r-n' \\ 1 + 2^{1-r}, & 若 4 \mid r-n' \end{cases}$

ii) 当$\tau > 0$时,

$$\partial_2(n) = 1 + \sum_{m=2}^{\infty} A_{2^m}(n)$$

$$= 1 + \sum_{m=2}^{\infty} 2^{-(m-1)r} C_{2^m}(2^{m-2}r - n)$$

$$= 1 + 2^{-(\tau+2-1)r} C_{2^{\tau+2}}(2^{\tau+2-2}r - 2^{\tau} n')$$

$$= 1 + 2^{-(\tau+1)r} C_{2^{\tau+2}}(2^{\tau}(r - n'))$$

$$= 1 + 2^{-(\tau+1)r} \cdot 2^{\tau} C_{2^2}(r - n')$$

$$= 1 + 2^{-(\tau+1)r+\tau} C_{2^2}(r - n')$$

$$= \begin{cases} 1 - 2^{(1-r)(\tau+1)}, & 若 2 \| r-n' \\ 1 + 2^{(1-r)(\tau+1)}, & 若 4 \mid r-n' \end{cases}$$

由i)、ii)立得

$$\partial_2(n) = \begin{cases} 1 - 2^{(1-r)(\tau+1)}, & 若 2 \| r-n' \\ 1 + 2^{(1-r)(\tau+1)}, & 若 4 \mid r-n' \end{cases}$$

引理3 如果$s = 2r$, $2 \nmid r$, $p > 2$, 并且$p^{\tau_1} \| n$, 则

$$\partial_p(n) = \left(1 - \frac{\chi(p)}{p^r}\right)\left(\frac{-1}{p^{\tau_1}}\right)(p^{\tau_1})^{1-r} \rho_{r-1}(p^{\tau_1})$$

因为 $\partial_p(n) = \sum_{l=0}^{\infty} A_{p^l}(n) = 1 + \sum_{l=1}^{\infty} A_{p^l}(n)$

$$A_{p^l}(n)=\sum_{\substack{a=1\\ p\nmid a}}^{p^l}\frac{1}{p^{sl}}\left(\sum_{x=1}^{p^l}e^{2\pi iax^2/p^l}\right)^s e^{-2\pi ian/p^l}$$

$$=\sum_{\substack{a=1\\ p\nmid a}}^{p^l}\frac{1}{p^{2rl}}\left(\sum_{x=1}^{p^l}e^{2\pi iax^2/p^l}\right)^{2r}e^{-2\pi ian/p^l}$$

又由第7章第5节定理6有

$$\sum_{x=1}^{p^l}e^{2\pi iax^2/p^l}=\begin{cases}\left(\frac{a}{p^l}\right)p^{\frac{l}{2}}, & 若p^l\equiv1(\bmod 4)\\ i\left(\frac{a}{p^l}\right)p^{\frac{l}{2}}, & 若p^l\equiv3(\bmod 4)\end{cases}$$

因此$\left(\sum_{x=1}^{p^l}e^{2\pi iax^2/p^l}\right)^{2r}=\begin{cases}p^{rl}, & 若p^l\equiv1\ (\bmod 4)\\ -p^{rl}, & 若p^l\equiv3\ (\bmod 4)\end{cases}$

此即 $\left(\sum_{x=1}^{p^l}e^{2\pi iax^2/p^l}\right)^{2r}=\left(\frac{-1}{p^l}\right)p^{rl}$

从而 $A_{p^l}(n)=\sum_{\substack{a=1\\ p\nmid a}}^{p^l}\frac{1}{p^{2rl}}\left(\frac{-1}{p^l}\right)p^{rl}e^{-2\pi ian/p^l}$

$$=\sum_{\substack{a=1\\ p\nmid a}}^{p^l}\frac{1}{p^{rl}}\left(\frac{-1}{p^l}\right)e^{-2\pi ian/p^l}$$

$$=\left(\frac{-1}{p^l}\right)\frac{1}{p^{rl}}C_{p^l}(n)$$

故 $\vartheta_p(n)=1+\sum_{l=1}^{\infty}\left(\frac{-1}{p^l}\right)p^{-rl}C_{p^l}(n)$

$$=1+\sum_{l=0}^{\tau_1}\left(\frac{-1}{p^l}\right)p^{-rl}\left(p^l-p^{l-1}\right)-p^{-r(\tau_1+1)}p^{\tau_1}\left(\frac{-1}{p^{\tau_1+1}}\right)$$

$$= \sum_{l=0}^{\tau_1}\left(\frac{-1}{p^l}\right)p^{-rl+l} - \sum_{l=1}^{\tau_1+1}\left(\frac{-1}{p^l}\right)p^{-rl+l-1}$$

$$= \left(1-\left(\frac{-1}{p}\right)p^{-r}\right)\sum_{l=1}^{\tau_1}\left(\frac{-1}{p^l}\right)p^{-(r-1)l}$$

$$= \left(1-\left(\frac{-1}{p}\right)p^{-r}\right)\sum_{l=1}^{\tau_1}\left(\frac{-1}{p^{\tau_1-l}}\right)p^{-(r-1)(\tau_1-l)}$$

$$= \left(1-\left(\frac{-1}{p}\right)p^{-r}\right)\left(p^{\tau_1}\right)^{1-r}\sum_{l=0}^{\tau_1}\left(\frac{-1}{p^{\tau_1-l}}\right)(p^l)^{r-1}$$

$$= \left(1-\left(\frac{-1}{p}\right)p^{-r}\right)\left(\frac{-1}{p^{\tau_1}}\right)\left(p^{\tau_1}\right)^{1-r}\sum_{l=0}^{\tau_1}\left(\frac{-1}{p^l}\right)(p^l)^{r-1}$$

$$= \left(1-\frac{\chi(p)}{p^r}\right)\left(\frac{-1}{p^{\tau_1}}\right)\left(p^{\tau_1}\right)^{1-r}\rho_{r-1}\left(p^{\tau_1}\right).$$

引理 4

$$L(r)\prod_p\left(1-\frac{\chi(p)}{p^r}\right)=1.$$

因为 $L(r)\prod\limits_p\left(1-\frac{\chi(p)}{p^r}\right)$

$$= \prod_p\left(1+\frac{\chi(p)}{p^r}+\frac{\chi(p^2)}{p^{2r}}+\frac{\chi(p^3)}{p^{3r}}+\cdots\right)\prod_p\left(1-\frac{\chi(p)}{p^r}\right)$$

$$= \prod_p\left(1+\frac{\chi(p^2)-\chi^2(p)}{p^{2r}}+\frac{\chi(p^3)-\chi(p^2)\chi(p)}{p^{3r}}+\cdots\right.$$

$$\left.+\frac{\chi(p^n)-\chi(p^{n-1})\chi(p)}{p^{nr}}+\cdots\right) \qquad (1)$$

又因为$p\equiv 1 \pmod 4$ 时，

$$p^n\equiv p^{n-1}\equiv 1 \pmod 4$$

$$\chi(p^n)=\chi(p^{n-1})=\chi(p)=1$$

当$p\equiv 3 \pmod 4$时，

$$p^n \equiv -p^{n-1} \pmod 4 ,$$

$$\chi(p) = -\chi(p^{n-1}) , \chi(p) = -1$$

此即对素数p，总有

$$\chi(p^n) - \chi(p^{n-1})\chi(p) = 0 ,\ n \geqslant 2 \qquad (2)$$

故由（1）、（2）可得

$$L(r)\prod_p\left(1 - \frac{\chi(p)}{p^r}\right) = 1$$

由以上引理可知，当$2\,\|\, r-n'$时，

$$L(r)\mathbf{S}_s(2^\tau n') = L(r)\prod_p \partial_p(n)$$

$$= (1 - 2^{(1-r)(\tau+1)})\left(\frac{-1}{n'}\right) n'^{1-r} \rho_{r-1}(n')$$

但$2\,\|\, r-n'$给出 $-\left(\frac{-1}{n'}\right) = \left(\frac{1}{r}\right)$

从而 $L(r) = \left(\left(\frac{-1}{n'}\right) + \left(\frac{-1}{r}\right) 2^{(1-r)(\tau+1)}\right) n'^{1-r} \rho_{r-1}(n')$.

当$4\,|\, r-n'$时，

$$L(r)\mathbf{S}_s(2^\tau n') = L(r)\prod_p \partial_p(n)$$

$$= (1 + 2^{(1-r)(\tau+1)})\left(\frac{-1}{n'}\right) n'^{1-r} \rho_{r-1}(n')$$

但$4\,|\, r-n'$给出 $\left(\frac{-1}{n'}\right) = \left(\frac{-1}{r}\right)$

从而也有

$$L(r) = \left(\left(\frac{-1}{n'}\right) + \left(\frac{-1}{r}\right) 2^{(1-r)(\tau+1)}\right) n'^{1-r} \rho_{r-1}(n').$$

故$s = 2r$，r为奇数时总有

$L(r)\mathbf{S}_S(2^\tau n')$

$$=\left(\left(\frac{-1}{n'}\right)+\left(\frac{-1}{r}\right)2^{(1-r)(\tau+1)}\right)n'^{1-r}\rho_{r-1}(n').$$

习题 2　证明

$$\delta_2(n)=2r_2(n).$$

证： 在求方程

$$x^2+y^2=n=2^\tau n',\quad 2\nmid n'$$

的整数解的组数时，总可假定$n'\equiv 1\pmod 4$。因为对任一组解x、y，可设$(x,y)=1$，从而x、y不能同时为偶数。

(a) 当x、y一奇一偶时，$\tau=0$，从

$$x^2+y^2\equiv 1\pmod 4$$

知有$n'\equiv 1\pmod 4$；

(b) 当x、y同为奇数时，由于$2\|x^2+y^2$，就有$\tau=1$，从而$n'\equiv 1\pmod 4$。因$n'\equiv 3\pmod 4$，给出$2\equiv 6\pmod 8$，此不可能。

引用习题 1 的记号，在本题中就有：

$s=2$。由$s=2r$，有$r=1$。

因为　$L(r)\mathbf{S}_S(2^\tau n')$

$$=\left(\left(\frac{-1}{n'}\right)+\left(\frac{-1}{r}\right)2^{(1-r)(\tau+1)}\right)n'^{1-r}\rho_{r-1}(n')$$

并且　$L(1)=\dfrac{\pi}{4}$

$n'^{1-r}=1$

$$\rho_{r-1}(n')=\rho_0(n')=\sum_{q\mid n'}\left(\frac{-1}{q}\right)=\sum_{q\mid n}\chi(q)$$

又因为$n'\equiv 1 \pmod 4$时，

$$\left(\left(\frac{-1}{n'}\right)+\left(\frac{-1}{r}\right)2^{(1-r)(\tau+1)}\right)=1+1=2$$

再注意到实密率

$$\partial_0(n)=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}-1\right)!}n^{\frac{s}{2}-1}=\pi$$

从$\delta_2(n)$的定义立刻得到

$$\delta_2(n)=\partial_0(n)\mathbf{S}_2(n)=\pi\mathbf{S}_2(n)$$

$$=\pi\cdot\frac{4}{\pi}\cdot 2\cdot\sum_{q|n}\chi(q)=2\left(4\sum_{q|n}\chi(q)\right)=2r_2(n).$$

习题3 证明

$$\delta_6(n)=16\sum_{d|n}\chi\left(\frac{n}{d}\right)d^2-4\sum_{d|n}\chi(d)d^2.$$

证：本题$s=6$，由$s=2r$得$r=3$。设$n=2^\tau n'$，$2\nmid n'$。因为

$L(r)\mathbf{S}_s(2^\tau n')$

$$=\left(\left(\frac{-1}{n'}\right)+\left(\frac{-1}{r}\right)2^{(1-r)(\tau+1)}\right)n'^{1-r}\rho_{r-1}(n')$$

并且 $L(3)=\frac{1}{1^3}-\frac{1}{3^3}+\frac{1}{5^3}-\cdots=\frac{\pi^3}{32}$

$$\left(\left(\frac{-1}{n'}\right)+\left(\frac{-1}{r}\right)^{(1-r)(\tau+1)}\right)=\left(\frac{-1}{n'}\right)-\frac{1}{4^{(\tau+1)}}$$

$$n'^{1-r}=\frac{1}{n'^2}$$

$$\rho_{r-1}(n')=\sum_{q|n}\left(\frac{-1}{q}\right)q^2$$

$$\partial_0(n)=\pi^{\frac{s}{2}}n^{\frac{s}{2}-1}\Big/\left(\frac{s}{2}-1\right)!=\frac{\pi^3}{2}n^2$$

故　$\delta_6(n)=\partial_0(n)\hat{S}_6(n)$

$$=\frac{\pi^3}{2}n^2\cdot\frac{32}{\pi^3}\left(\left(\frac{-1}{n'}\right)-\frac{1}{4^{(\tau+1)}}\right)\frac{1}{n'^2}\sum_{q|n'}\left(\frac{-1}{q}\right)q^2$$

$$=16\cdot4^{\tau}\left(\frac{-1}{n'}\right)\sum_{q|n'}\left(\frac{-1}{q}\right)q^2-4\sum_{q|n'}\left(\frac{-1}{q}\right)q^2.$$

又因　$4^{\tau}\left(\frac{-1}{n'}\right)\sum_{q|n'}\left(\frac{-1}{q}\right)q^2=\sum_{q|n'}\left(\frac{-1}{n'/q}\right)\left(\frac{-1}{q}\right)^2(2^{\tau}q)^2$

$$=\sum_{q|n'}\left(\frac{-1}{n'/q}\right)(2^{\tau}q)^2=\sum_{d|n}\chi\left(\frac{n}{d}\right)d^2$$

且　$\sum_{q|n'}\left(\frac{-1}{q}\right)q^2=\sum_{d|n}\chi(d)d^2$

所以　$\delta_6(n)=16\sum_{d|n}\chi\left(\frac{n}{d}\right)d^2-4\sum_{d|n}\chi(d)d^2.$

第九章　素数定理

一、提　　要

定义　设$x>0$，令

$$\theta(x)=\sum_{p\leqslant x}\log p,$$

$$\psi(x)=\sum_{n\leqslant x}\Lambda(n)=\sum_{p^m\leqslant x}\log p.$$

容易得到

$$\psi(x)=\theta(x)+\theta(x^{\frac{1}{2}})+\theta(x^{\frac{1}{3}})+\cdots$$

$$\psi(x)=\sum_{p\leqslant x}\left[\frac{\log x}{\log p}\right]\log p.$$

定理 1

$$\pi(x)\sim\frac{x}{\log x}.$$

此定理称为素数定理。

定理 2

$$\lim_{x\to\infty}\frac{\pi(x)}{x(\log x)^{-1}}=\lim_{x\to\infty}\frac{\theta(x)}{x}=\lim_{x\to\infty}\frac{\psi(x)}{x}$$

由定理 2 可知，若要证明素数定理，只需证明

$$\psi(x)\sim x$$

或 $$\theta(x)\sim x$$

定义 用$s=\sigma+it$表一复数，σ及t为实数，级数

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}\quad(\sigma>1)$$

称为Riemann ζ函数。

定理3 当$\sigma\geqslant a>1$时，$\zeta(s)$是一致收敛的。

定理4 设$x>1$，则

$$\theta(x)\log x+\sum_{p\leqslant x}\theta\left(\frac{x}{p}\right)\log p=2x\log x+O(x),$$

$$\sum_{p\leqslant x}\log^2 p+\sum_{pq\leqslant x}\log p\log q=2x\log x+O(x).$$

定理5 若$k>0$，$l>0$，$(k,l)=1$，则形如$kn+l$的素数个数无穷。

定理6 若$k>0$，$l>0$，则

$$\sum_{\substack{p\leqslant x\\ p\equiv l(\mathrm{mod}k)}}\frac{\log p}{p}=\frac{1}{\varphi(k)}\log x+O(1).$$

此处和号表示对所有不超过x的形如$kn+l$的素数求和；与O有关的常数仅与k有关。显然，定理6较定理5强些。

若用$\pi(x;k,l)$表示在等差数列$kn+l$中不超过x的素数个数，则现在已经证明了：

对任意固定的正常数A，如果设$k\leqslant\log^A x$，则

$$\pi(x;k,l)=\frac{\mathrm{li}x}{\varphi(k)}+O(xe^{-c\sqrt{\log x}})$$

其中c为一正常数．此定理是解析数论中的一个重要定理，它是经过许多数学家的努力才得到的，是研究Goldbach猜想的基本定理．

关于素数定理也有很多改进，例如在许多数学家的努力下得到了

$$\pi(x)=\text{li}\,x+O\left(e^{-c\log^{\frac{3}{5}}x(\log\log x)^{-\frac{1}{5}}}\right)$$

其中C为正常数.

二、题　　解

§5　素数定理

习题1　设p_n表示第n个素数. 试用素数定理证明

$$\lim_{n\to\infty}\frac{p_n}{n\log n}=1.$$

反之，由此也可以推出素数定理.

证：在定理1中取$x=p_n$得

$$n=\pi(p_n)\sim\frac{p_n}{\log p_n}$$

此即　$p_n\sim n\log p_n$　　(1)

又因为　$\log\log p_n=O(\log p_n)$

所以　$\log p_n\sim\log n+\log\log p_n\sim\log n$　　(2)

把(2)代入(1)立得　$\lim\limits_{n\to\infty}\frac{p_n}{n\log n}=1$　　(3)

下面再证明，如果(3)成立，则定有$\pi(x)\sim\frac{x}{\log x}$.

设$p_n\leqslant x<p_{n+1}$，则

$$n=\pi(p_n)\leqslant\pi(x)<\pi(p_{n+1})=n+1$$

故有　$\frac{n}{p_{n+1}}<\frac{\pi(x)}{x}<\frac{n+1}{p_n}$　　(4)

(3)式给出　$p_{n+1}\sim(n+1)\log(n+1)\sim n\log n$

$$p_n \sim n\log n \sim (n+1)\log n$$

即
$$\frac{n}{p_{n+1}} \sim \frac{1}{\log n}$$

$$\frac{n+1}{p_n} \sim \frac{1}{\log n}$$

把上面二式代入（4）得

$$\frac{\pi(x)}{x} \sim \frac{1}{\log n} \tag{5}$$

又从$p_n \leqslant x < p_{n+1}$可得

$$\log p_n \leqslant \log x < \log p_{n+1} \tag{6}$$

由（2）得 $\log p_n \sim \log p_{n+1} \sim \log n$

从而（6）给出 $\log x \sim \log n$,

结合（5）得
$$\frac{\pi(x)}{x} \sim \frac{1}{\log x}$$

此即
$$\pi(x) \sim \frac{x}{\log x}.$$

习题 2 试由素数定理推出

$$M(x) = \sum_{n \leqslant x} \mu(n) = o(x).$$

证：因为

$$\Lambda(n) = \sum_{d \mid n} \mu(d)\log\frac{n}{d} = \log n \sum_{d \mid n} \mu(d) - \sum_{d \mid n} \mu(d)\log d$$

$$= -\sum_{d \mid n} \mu(d)\log d$$

从而$-\mu(n)\log n$是$\Lambda(n)$的Möbius逆变换，所以

$$-\mu(n)\log n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right)\Lambda(d) \tag{1}$$

因为对任意的$h>0$、$n \geqslant 2$都有

$$\log^h \frac{x}{n} \leqslant \int_{n-1}^{n} \log^h \frac{x}{t} dt$$

因此 $\displaystyle\sum_{n=2}^{[x]} \log^h \frac{x}{n} \leqslant \int_1^x \log^h \frac{x}{t}\, dt = x\int_1^x \frac{\log^h u}{u^2} du$

$$< x\int_1^{\infty} \frac{\log^h u}{u^2} du = Ax$$

所以 $\displaystyle\sum_{n\leqslant x} \log^h \frac{x}{n} = O(x)$，$(h>0)$

故 $\displaystyle\sum_{n\leqslant x} \mu(n) \log \frac{x}{n} = O\left(\sum_{n\leqslant x} \log \frac{x}{n}\right) = O(x)$

即 $\displaystyle M(x)\log x = \sum_{n\leqslant x} \mu(n) \log n + O(x)$ （2）

命 $\psi(x) = x + R(x)$ （3）

则由素数定理 $\psi(x) \sim x$

可得 $R(x) = o(x)$ （4）

由（1）、（4）得

$$-\sum_{n\leqslant x} \mu(n)\log n = \sum_{n\leqslant x} \sum_{d\mid n} \mu\left(\frac{n}{d}\right) \Lambda(d)$$

$$= \sum_{dk\leqslant x} \mu(k)\Lambda(d) = \sum_{k\leqslant x} \mu(k)\psi\left(\frac{x}{k}\right)$$

$$= \sum_{k\leqslant x} \mu(k)\psi\left(\left[\frac{x}{k}\right]\right)$$

$$= \sum_{k\leqslant x} \mu(k)\left[\frac{x}{k}\right] + \sum_{k\leqslant x} \mu(k) R\left(\left[\frac{x}{k}\right]\right) \qquad (5)$$

因为 $\displaystyle\sum_{k\leqslant x} \mu(k)\left[\frac{x}{k}\right] = \sum_{n\leqslant x} \sum_{k\mid n} \mu(k) = 1$ （6）

又从（4）可知，任给 $\varepsilon>0$，都存在正常数 N，当 $x\geqslant N$ 时，

$|R(x)|<\varepsilon x$。而从定理9.1.2易证，存在正数B，对于$x\geqslant 1$，总有$|R(x)|<Bx$，

因此
$$\left|\sum_{k\leqslant x}\mu(k)R\left(\left[\frac{x}{k}\right]\right)\right|\leqslant\sum_{k\leqslant x}\left|R\left(\left[\frac{x}{k}\right]\right)\right|$$
$$\leqslant\sum_{k\leqslant x/N}\varepsilon\left[\frac{x}{x}\right]+\sum_{x/N<k\leqslant x}B\left[\frac{x}{k}\right]$$
$$\leqslant\varepsilon x\log\frac{x}{N}+Bx\left(\log x-\log\frac{x}{N}\right)+O(x)$$
$$=\varepsilon x\log x+O(x).$$

由于ε可以任意小，从而上式给出
$$\sum_{k\leqslant x}\mu(k)R\left(\left[\frac{x}{k}\right]\right)=o(x\log x) \qquad (7)$$

把（6）、（7）代入（5）得
$$-\sum_{n\leqslant x}\mu(n)\log n=o(x\log x)$$

再由（2）得 $-M(x)\log x=o(x\log x)$

故 $M(x)=o(x)$。
$$M(x)=O(xe^{-c\sqrt{\log x}})\ *$$
$$M(x)=O\left(xe^{-c\log^{\frac{3}{5}-\varepsilon}x}\right)$$
$$|M(x)|<\sqrt{x},\quad x>1.**$$

习题3 试由素数定理推出
$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n}=0.$$

证： 设p_1，p_2，…，$p_{\pi(N)}$是不超过正整数N的所有素数，

---

* 《解析数论基础》（长拉楚巴著）第50页和第73页指出.

** Merten猜测.

a_i（$1\leqslant i\leqslant\pi(N)$）是合条件$p_i^{a_i}\leqslant N$、$p_i^{a_i+1}>N$的正整数，$P_N$是无穷乘积

$$P=\prod_{i=1}^{\infty}\left(1-\frac{1}{p_i}\right)$$

的前N项积，即$P_N=\prod\limits_{i=1}^{N}\left(1-\frac{1}{p_i}\right)$

由定理5.4.5　　$P=0$

可得　　　　　$\lim\limits_{N\to\infty}P_N=0$.

从素数定理$\pi(N)\sim\dfrac{N}{\log N}$知，$N\to\infty$时，必定有$\pi(N)\to\infty$，因此

$\{P_{\pi(N)}\}$是$\{P_N\}$的一个子列。从而有

$$\lim_{N\to\infty}P_{\pi(N)}=0 \tag{1}$$

显然，$P_{\pi(N)}$可以写成

$$P_{\pi(N)}=\prod_{i=1}^{\pi(N)}\left(1-\frac{1}{p_i}\right)$$

$$=\prod_{i=1}^{\pi(N)}\left(1+\frac{\mu(p_i)}{p_i}+\frac{\mu(p_i^2)}{p_i^2}+\cdots+\frac{\mu\left(p_i^{a_i}\right)}{p_i^{a_i}}\right)$$

$$=1+\frac{\mu(2)}{2}+\frac{\mu(3)}{3}+\cdots+\frac{\mu(N)}{N}$$

$$+\frac{\mu(N_1)}{N_1}+\frac{\mu(N_2)}{N_2}+\cdots+\frac{\mu\left(p_1^{a_1}\cdots p_{\pi(N)}^{a_{\pi(N)}}\right)}{p_1^{a_1}\cdots p_{\pi(N)}^{a_{\pi(N)}}} \tag{2}$$

且合条件

$$1<2<3<\cdots<N<N_1\cdots<p_1^{a_1}\cdots p_{\pi(N)}^{a_{\pi(N)}} \tag{3}$$

因为p_1，…，$p_{\pi(N)}$是不超过N的所有素数，所以（2）式右边前N项和就是$\sum_{n=1}^{N}\frac{\mu(n)}{n}$。如果设

$$R(N)=\frac{\mu(N_1)}{N_1}+\frac{\mu(N_2)}{N_2}+\cdots+\frac{\mu\left(p_1^{\alpha_1}\cdots p_{\pi(N)}^{\alpha_{\pi(N)}}\right)}{p_1^{\alpha_1}\cdots p_{\pi(N)}^{\alpha_{\pi(N)}}}$$

那么（2）式可以写成

$$\sum_{n=1}^{N}\frac{\mu(n)}{n}=P_{\pi(N)}-R(N). \tag{2'}$$

由（3）容易推出

$$\lim_{N\to\infty}R(N)=0 \tag{4}$$

故把（2′）式两边取极限并利用（1）、（4）可得

$$\lim_{N\to\infty}\sum_{n=1}^{N}\frac{\mu(n)}{n}=\lim_{N\to\infty}\left(P_{\pi(N)}-R(N)\right)$$
$$=\lim_{N\to\infty}P_{\pi(N)}-\lim_{N\to\infty}R(N)=0$$

此即 $$\sum_{n=1}^{\infty}\frac{\mu(n)}{n}=0$$

习理4　设$n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，定义

讨论：利用$Abel$变换可以证明：若$\sum_{n=1}^{\infty}\frac{\mu(n)}{n}=0$，则$M(x)=o(x)$，而《*Introduction to Analytic Namber Theory*》一书第94页又指出：$M(x)=o(x)$可以推出$\psi(x)\sim x$，因此素数定理，$M(x)=o(x)$以及$\sum_{n=1}^{\infty}\frac{\mu(n)}{n}=0$是等价的。

$$\omega(n)=k,\quad \Omega(n)=a_1+a_2+\cdots+a_k.$$

命 $$\pi_k(x)=\sum_{\substack{n\leqslant x\\ \omega(n)=\Omega(n)=k}}1,\quad \tau_k(x)=\sum_{n\leqslant x}1,$$

$$\theta_k(x)=\sum_{p_1\cdots p_k\leqslant x}\log(p_1\cdots p_k),\quad \prod_k(x)=\sum_{p_1\cdots p_k\leqslant x}1$$

（注意：此处之求和号表示过素数p_1，…，p_k，而具有性质$p_1\cdots p_k\leqslant x$者；同一组p_1，…，p_k若次序不同亦算作不同）

试证：

$$\prod_k(x)\sim\frac{kx(\log\log x)^{k-1}}{\log x}\qquad(k\geqslant 2),$$

$$\theta_k(x)\sim kx(\log\log x)^{k-1}\qquad(k\geqslant 2),$$

$$\pi_k(x)\sim\tau_k(x)\sim\frac{x(\log\log x)^{k-1}}{(k-1)!\log x}\qquad(k\geqslant 2).$$

证：以Cn表示

$$n=p_1\cdots p_k\qquad(1)$$

所能表出的个数，则有

$$\prod_k(x)=\sum_{n\leqslant x}Cn,\quad \theta_k(x)=\sum_{n\leqslant x}Cn\log n$$

如果（1）中的p均不同，则$Cn=k!$（在任何情形下均有$Cn\leqslant k!$）。如n不是（1）的形状，则$Cn=0$。故

$$k!\,\pi_k(x)\leqslant\prod_k(x)\leqslant k!\,\tau_k(x)\qquad(k\geqslant 1)\qquad(2)$$

对于$k\geqslant 2$，考虑n表成（1）的形状时至少有两个p相等的情形，这些$n\leqslant x$的个数是

$$\tau_k(x)-\pi_k(x)$$

每一个这种n都可以用$p_{k-1}=p_k$表成（1）的形状，故有

$$\tau_k(x)-\pi_k(x)\leqslant\sum_{p_1p_2\cdots p^2_{k-1}\leqslant x}1\leqslant\sum_{p_1\cdots p_{k-1}\leqslant x}1$$

$$= \prod_{k-1}(x) \qquad (3)$$

（3）中$k \geqslant 2$。

我们将在后面证明

$$\theta_k(x) \sim kx(\log\log x)^{k-1}, \ (k \geqslant 2) \qquad (4)$$

$$\theta_k(x) = \sum_{n \leqslant x} C n \log n = \prod_k(1)\log 1 + \left\{\prod_k(2) - \prod_k(1)\right\}\log 2$$

$$+ \cdots + \left\{\prod_k\left([x]\right) - \prod_k\left([x] - 1\right)\right\}\log [x]$$

$$= \prod_k(1)\left\{\log 1 - \log 2\right\} + \cdots + \prod_k\left([x]\right.$$

$$\left.- 1\right)\left\{\log\left([x] - 1\right) - \log[x]\right\}$$

$$+ \prod_k\left([x]\right)\log[x].$$

当$x \leqslant t < n+1$时，$\prod_k(t) = \prod_k(n)$，故有

$$\prod_k(n)\left\{\log n - \log(n+1)\right\} = -\int_n^{n+1} \prod_k(t)(\log t)' dt$$

即得　$$\theta_k(x) = \prod_k(x)\log x - \int_2^x \frac{\prod_k(t)}{t} dt$$

今有 $\tau_k(x) \leqslant x$，由（2）得$\prod_k(t) = O(t)$和

$$\int_2^x \frac{\prod_k(t)}{t} dt = O(x)$$

故对$k \geqslant 2$，由（4）得出

$$\prod_k(x) = \frac{\theta_k(x)}{\log x} + O\left(\frac{\log x}{x}\right) \sim \frac{kx(\log\log x)^{k-1}}{\log x} \qquad (5)$$

因 $\prod_1(x) = \pi(x)$此对$k = 1$亦成立。用(5) 式代入(2)和(3)，

即得

$$\pi_k(x)\sim\tau_k(x)\sim\frac{x(\log\log x)^{k-1}}{(k-1)!\log x}\qquad(k\geqslant 2).$$

现在来证明（4）式，对所有$k\geqslant 1$，

$$k\theta_{k+1}(x)=\sum_{p_1\cdots p_{k+1}\leqslant x}\{\log(p_2p_3\cdots p_{k+1})$$

$$+\log(p_1p_3\cdots p_{k+1})+\cdots+\log(p_1p_2\cdots p_k)\}$$

$$=(k+1)\sum_{p_1\cdots p_{k+1}\leqslant x}\log(p_2p_3\cdots p_{k+1})$$

$$=(k+1)\sum_{p_1\leqslant x}\theta_k\left(\frac{x}{p_1}\right)$$

设 $L_0(x)=1$，$L_k(x)=\sum_{p_1\cdots p_k\leqslant x}\frac{1}{p_1\cdots p_k}$

$$=\sum_{p_1\leqslant x}\frac{1}{p_1}L_{k-1}\left(\frac{x}{p_1}\right),$$

故如写

$$f_k(x)=\theta_k(x)-kxL_{k-1}(x),$$

则有

$$kf_{k+1}(x)=(k+1)\sum_{p\leqslant x}f_k\left(\frac{x}{p}\right),\qquad(6)$$

用此进行归纳法来证明

$$f_k(x)=o\{x(\log\log x)^{k-1}\},\quad(k\geqslant 1).\qquad(7)$$

首先，因

$$f_1(x)=\theta_1(x)-x=\theta(x)-x=o(x),$$

故（7）对$k=1$成立．设$k=K\geqslant 1$成立，对于任意$\varepsilon>0$，有$x_0=x_0(K,\varepsilon)$存在使得对于所有$x\geqslant x_0$，均有

$$|f_K(x)|<\varepsilon x(\log\log x)^{K-1}$$

由$f_K(x)$的定义，对于$1\leqslant x<x_0$，有

$$|f_K(x)|<D$$

其中，D只同K和ε有关，故对足够大的x，有

$$\sum_{p\leqslant x/x_0}\left|f_K\left(\frac{x}{p}\right)\right|<\varepsilon(\log\log x)^{K-1}\sum_{p\leqslant x/x_0}\frac{x}{p}$$

$$<2\varepsilon x(\log\log x)^K$$

$\left(\text{用及}\ \sum_{p\leqslant x}\frac{1}{p}=\log\log x+C+o(1)\right)$

再者，$\sum_{x/x_0<p\leqslant x}\left|f_K\left(\frac{x}{p}\right)\right|<D\pi(x)<Dx$

故由（6），从$K+1\leqslant 2K$，得出对于$x>x_1=x_1(\varepsilon,\ D,\ K)=x_1(\varepsilon,\ K)$，有

$$|f_{K+1}(x)|<2x\{2\varepsilon(\log\log x)^K+D\}<5\varepsilon x(\log\log x)^K$$

因ε是任意取的，这就得出（7）式，知（7）式对所有$k\geqslant 1$成立。

只要证明

$$L_k(x)\sim(\log\log x)^k,\ (k\geqslant 1) \qquad (8)$$

由（7）即可证明（4）式。在（1）中，如每一个$p_i\leqslant x^{1/K}$，则有$n\leqslant x$；反之，如$n\leqslant x$，则对每一个i均有$p_i\leqslant x$，故

$$\left(\sum_{p\leqslant x^{1/x}}\frac{1}{p}\right)^k\leqslant L_k(x)\leqslant\left(\sum_{p\leqslant x}\frac{1}{p}\right)^k$$

但因

$$\sum_{p\leqslant x}\frac{1}{p}\sim\log\log x$$

$$\sum_{p\leqslant x^{1/k}}\frac{1}{p}\sim\log\left(\frac{\log x}{k}\right)\sim\log\log x$$

故即得出（8）式，证毕。

上面给出的

$$\prod_k(x)\sim\frac{kx(\log\lg x)^{k-1}}{\log x},\ (k\geqslant 2) \qquad (5)$$

和 $$\pi_k(x)\sim\tau_k(x)\sim\frac{x(\log\lg x)^{k-1}}{(k-1)!\log x}\quad (k\geqslant 2)\qquad (9)$$

的证明，是利用了

$$\theta_k(x)\sim kx(\log\lg x)^{k-1},\qquad (k\geqslant 2)\qquad (4)$$

而得到的。下面再给出（5）和（9）的一种证明，此种证明并不利用（4）式。

引理 $F(u, x)$是u，x，$2\leqslant u<x$的函数，满足

1）$F(u, x)\geqslant 0$；

2）对给定的$x>2$，u从2至x时，$F(u, x)/\log u$不是上升函数；

3）$F(2, x)=o\left(\int_2^x\frac{F(u,x)}{\log u}du\right)$

则 $$\sum_{p\leqslant x}F(p, x)\sim\int_2^x\frac{F(u,x)}{\log u}du$$

证：设$\theta(x)=\sum\limits_{p\leqslant x}\log p$，当$x\geqslant 2$时，写$\theta(x)=x+x\varepsilon(x)$，

$\varepsilon(x)=o(1)$，则有

$$\sum_{p\leqslant x}F(p, x)=\sum_{n=2}^{x}\frac{\theta(n)-\theta(n-1)}{\log n}F(n, x)$$

$$=\sum_{n=2}^{x}\frac{1}{\log n}F(n,x)+\sum_{n=2}^{x}\frac{n\varepsilon(n)-(n-1)\varepsilon(n-1)}{\log n}F(n,x)$$

$$=\sum_{n=2}^{x}\frac{F(n,x)}{\log n}+\sum_{n=2}^{x-1}n\varepsilon(n)\left(\frac{F(n,x)}{\log n}-\frac{F(n+1,x)}{\log(n+1)}\right)$$

$$+\frac{F(2,x)}{\log 2}+[x]\varepsilon([x])\frac{F([x],x)}{\log[x]}.$$

由假设 $$\sum_{n=2}^{x}\frac{F(n,x)}{\log n}+\frac{F(2,x)}{\log 2}=\int_2^x\frac{F(u,x)}{\log u}du$$

$$+o\left(\int_2^x \frac{F(u,x)}{\log u}du\right)$$

取$\delta>0$，对所有$u\geqslant\omega=\omega(\delta)$,

$$|\varepsilon(u)|<\delta.$$

故对$x\geqslant 2$，$x\geqslant\omega+1$，

$$\left|\sum_{n=2}^{x-1} n\varepsilon(n)\left(\frac{F(n,x)}{\log n}-\frac{F(n+1,x)}{\log(n+1)}\right)+[x]\varepsilon([x])\frac{F([x],x)}{\log[x]}\right|$$

$$<O(F(2,x))+\delta\sum_{n=\omega}^{x-1} n\left(\frac{F(n,x)}{\log n}-\frac{F(n+1,x)}{\log(n+1)}\right)$$

$$+\delta[x]\frac{F([x],x)}{\log[x]}$$

$$=\delta\sum_{n=\omega}^{x}\frac{F(n,x)}{\log n}+O(F(2,x))$$

$$\leqslant\delta\int_2^x\frac{F(u,x)}{\log u}du+o\left(\int_2^x\frac{F(u,x)}{\log u}du\right)$$

因δ是任意取的，故有

$$\sum_{n=2}^{x-1} n\varepsilon(n)\left(\frac{F(n,x)}{\log n}-\frac{F(n+1,x)}{\log(n+1)}\right)+[x]\varepsilon([x])\frac{F([x],x)}{\log[x]}$$

$$=o\left(\int_2^x\frac{F(u,x)}{\log u}du\right)$$

故得
$$\sum_{p\leqslant x}F(p,x)=\int_2^x\frac{F(u,x)}{\log u}du+o\left(\int_2^x\frac{F(u,x)}{\log u}du\right)$$
$$\sim\int_2^x\frac{F(u,x)}{\log u}du.$$

$\pi_k(x)$为$\leqslant x$的无平方因子数的个数。下面用归纳法证明

$$\pi_k(x)\sim\frac{1}{(k-1)!}\cdot\frac{x(\log\log x)^{k-1}}{\log x} \tag{10}$$

$k=2$，即求$pq\leqslant x$的解的个数，素数$p\neq q$，$2\pi_2(x)=\sum\limits_{p\leqslant x}\pi\left(\frac{x}{p}\right)-\pi(\sqrt{x})$，其中$\sum\limits_{p\leqslant x}\pi\left(\frac{x}{p}\right)$为$pq\leqslant x$的解的个数，$p\neq q$；$\pi(\sqrt{x})$为$p=q$的解的个数，故有

$$2\pi_2(x)=\sum_{p\leqslant x}\pi\left(\frac{x}{p}\right)+O\left(\frac{\sqrt{x}}{\log x}\right)$$

取 $F(p,x)=\pi\left(\frac{x}{p}\right)$，则

1）对$2\leqslant u\leqslant x$，$\pi\left(\frac{x}{u}\right)\geqslant 0$；

2）给定x，$\pi\left(\frac{x}{u}\right)\Big/\log u$对$u\geqslant 2$时不上升；

3）$\pi\left(\frac{x}{2}\right)=o\left(\int_2^x\frac{F(u,x)}{\log u}du\right)$，即是

$$\frac{x}{\log x}=o\left(\int_2^x\frac{\pi\left(\frac{x}{u}\right)}{\log u}du\right)$$

$$\int_2^x\frac{\pi\left(\frac{x}{u}\right)}{\log u}du=\int_2^{\frac{x}{2}}\frac{\pi\left(\frac{x}{u}\right)}{\log u}du=x\int_2^{\frac{x}{2}}\frac{\pi(v)}{\log x-\log v}\cdot\frac{dv}{v^2}$$

$\delta>0$，$v\geqslant\omega=\omega(\delta)$，$\left|\pi(v)-\frac{v}{\log v}\right|<\delta\frac{v}{\log v}$

$x>2\omega$时，

$$\left|\int_\omega^{\frac{x}{2}}\frac{\pi(v)}{\log x-\log v}\cdot\frac{dv}{v^2}-\int_\omega^{\frac{x}{2}}\frac{v/\log v}{\log x-\log v}\cdot\frac{dv}{v^2}\right|$$

$$<\delta\int_\omega^{\frac{x}{2}}\frac{v/\log v}{\log x-\log v}\cdot\frac{dv}{v^2}$$

$$\left|\int_2^{\frac{x}{2}}\frac{\pi(v)}{\log x-\log v}\cdot\frac{dv}{v^2}-\int_2^{\frac{x}{2}}\frac{\frac{v}{\log v}}{\log x-\log v}\cdot\frac{dv}{v^2}\right|$$

$$<'\delta\int_2^{\frac{x}{2}}\frac{\frac{v}{\log v}}{\log x-\log v}\cdot\frac{dv}{v^2}+O\left(\frac{1}{\log x}\right).$$

由于

$$\int_2^{\frac{x}{2}}\frac{\frac{v}{\log v}}{\log x-\log v}\cdot\frac{dv}{v^2}=\int_{\log 2}^{\log x-\log 2}\frac{d\omega}{\omega(\log x-\omega)}=\frac{1}{\log x}\cdot$$

$$\int_{\log 2}^{\log x-\log 2}\left(\frac{1}{\omega}+\frac{1}{\log x-\omega}\right)d\omega$$

$$=\frac{1}{\log x}\left\{\log(\log x-\log 2)-\log\log 2-\log\log 2+\log(\log x-\log 2)\right\},$$

$$\sim\frac{2\log\log x}{\log x},$$

故对足够大的x，有

$$\left|\frac{\int_2^{\frac{x}{2}}\frac{\pi(v)}{\log x-\log v}\cdot\frac{dv}{v^2}}{\int_2^{\frac{x}{2}}\frac{\frac{v}{\operatorname{tg}v}}{\log x-\log v}\cdot\frac{dv}{v^2}}-1\right|<\delta+\delta=2\delta$$

即

$$\int_2^{\frac{x}{2}}\frac{\pi(v)}{\log x-\log v}\cdot\frac{dv}{v^2}\sim\int_2^{\frac{x}{2}}\frac{\frac{v}{\lg v}}{\log x-\log v}\cdot\frac{dv}{v^2}\sim\frac{2\log\log x}{\log x}$$

$$\int_2^x\frac{\pi\left(\frac{x}{u}\right)}{\log u}du\sim\frac{2x\log\log x}{\log x}$$

故有 $\pi_2(x) \sim \frac{x\log\log x}{\log x}$

设 $\pi_k(x) \sim \frac{1}{(k-1)!} \frac{x(\log\log x)^{k-1}}{\log x}$

次计算$pQ \leqslant x$的解的个数。Q是无平方因子数，有k个素因子，此数为

$$\sum_{p \leqslant x} \pi_k\left(\frac{x}{p}\right) = (k+1)\pi_{k+1}(x) + g(x)$$

另一方面，$g(x)$为$\leqslant x$，且有$k-1$个素因子的数的个数，每个计算了两次。

$$g(x) = O\left(\sum_{p \leqslant \sqrt{\frac{x}{2}}} \pi_{k-1}\left(\frac{x}{p^2}\right)\right)$$

$$= O\left(\sum_{n=1}^{\sqrt{\frac{x}{2}}} \pi_{k-1}\left(\frac{x}{n^2}\right)\right)$$

$$= O\left(\sum_{n=1}^{\sqrt{\frac{x}{2}}} \frac{x}{n^2} \cdot \frac{(\log\log x)^{k-2}}{\log\frac{x}{n^2}}\right)$$

$$= O\left(x(\log\log x)^{k-2} \sum_{n=2}^{\sqrt{\frac{x}{2}}} \frac{1}{n^2 \lg\frac{x}{n^2}}\right)$$

由于

$$\sum_{n=1}^{\sqrt{\frac{x}{2}}} \frac{1}{n^2 \log\frac{x}{n^2}} = O\left(\sum_{n=1}^{\sqrt[4]{x}} \frac{1}{n^2} \cdot \frac{1}{\lg\frac{x}{\sqrt{x}}}\right) +$$

$$O\left[\sum_{n=\sqrt[4]{x}+1}^{\sqrt{\frac{x}{2}}}\frac{1}{n^2}\cdot\frac{1}{\log 2}\right]$$

$$=O\left(\frac{1}{\log x}\right)+O\left(\frac{1}{\sqrt[4]{x}}\right)=O\left(\frac{1}{\log x}\right)$$

$$g(x)=O\left(\frac{x(\log\log x)^{k-2}}{\log x}\right)=O(\pi_k(x))$$

$$(k+1)\pi_{k+1}(x)\sim\sum_{p\leqslant x}\pi_k\left(\frac{x}{p}\right)$$

由假设3

$$\frac{x(\log\log x)^{k-1}}{\lg x}=O\left[\int_2^x\frac{\pi_k\left(\frac{x}{u}\right)}{\log u}du\right]$$

$$(k+1)\pi_{k+1}(x)\sim\int_2^{\frac{x}{2}}\frac{\pi_k\left(\frac{x}{u}\right)}{\log u}du=$$

$$=x\int_2^{\frac{x}{2}}\frac{\pi_k(v)}{\log x-\log v}\cdot\frac{dv}{v^2}$$

$$\sim x\int_2^{\frac{x}{2}}\frac{v(\log\log v)^{k-1}}{(k-1)!\log v}\cdot\frac{dv}{(\log x-\log v)v^2}$$

$\Big[\delta>0$，$v\geqslant\omega=\omega(\delta)$，

$$\left|\pi_k(v)-\frac{v(\log\log v)^{k-1}}{(k-1)!\log v}\right|<\delta\cdot\frac{v(\log\log v)^{k-1}}{(k-1)!\log v},$$

在上式积分中换$\pi_k(v)$为$\frac{v(\log\log v)^{k-1}}{(k-1)!\log v}$，其误差

$$<O\left(\frac{1}{\log x}\right)+\delta\int_2^{\frac{x}{2}}\frac{v(\log\log v)^{k-1}dv}{(k-1)!\log v(\log x-\log v)v^2}\Big]$$

$$\frac{(k-1)!\,(k+1)\pi_{k+1}(x)}{x} \sim \int_2^{\frac{x}{2}} \frac{(\log\log v)^{k-1}\,dv}{v\log v\,(\log x-\log v)}$$

$$= \int_{\log 2}^{\log x-\log 2} \frac{\log^{k-1}\omega d\omega}{\omega(\log x-\omega)} = \int_1^{\log x-1} \frac{\log^{k-1}\omega d\omega}{\omega(\log x-\omega)} + O\left(\frac{(\log\log x)^{k-1}}{\log x}\right)$$

$$= \frac{1}{\log x}\int_1^{\log x-1} \frac{\log^{k-1}\omega}{\omega} d\omega + \frac{1}{\log x}\int_1^{\log x-1} \frac{\log^{k-1}\omega}{\log x-\log\omega} d\omega$$

$$+O\left(\frac{(\log\log x)^{k-1}}{\log x}\right),$$

$$\int_1^{\log x-1} \frac{\log^{k-1}\omega}{\omega} d\omega = \frac{1}{k}\Big(\log(\log x-1)\Big)^k \sim \frac{1}{k}(\log\log x)^k;$$

$$\int_1^{\log x-1} \frac{\log^{k-1}\omega}{\log x-\omega} d\omega = \int_1^{\log\frac{x}{2}} \frac{\log^{k-1}\omega}{\log x-\omega} d\omega + \int_{\log\frac{x}{2}}^{\log x-1}$$

$$\frac{\log^{k-1}\omega}{\log x-\omega} d\omega = O\left(\log x\frac{(\log\log x)^{k-1}}{\log x}\right) + \log^{k-1}\Big(\log x-$$

$$-\frac{\Theta}{2}\log x\Big)\int_{\log\frac{x}{2}}^{\log x-1} \frac{d\omega}{\log x-\omega}$$

其中 $0<\Theta\leqslant 1$.

由于 $\log^{k-1}\left(\log x-\frac{\Theta}{2}\log x\right)\sim(\log\log x)^{k-1}$

$$\int_{\log\frac{x}{2}}^{\log x-1}\frac{d\omega}{\log x-\omega}=\log\frac{\log x-\frac{\log x}{2}}{\log x-(\log x-1)}=\log\frac{\log x}{2}\sim\log\log x$$

$$\int_{1}^{\log x-1}\frac{\log^{k-1}\omega}{\log x-\omega}d\omega\sim(\log\log x)^k$$

故

$$\frac{(k-1)!\,(k+1)\pi_{k+1}(x)}{x}\sim\left(\frac{1}{k}+1\right)\frac{(\log\log x)^k}{\log x}$$

$$\pi_{k+1}(x)\sim\frac{1}{k!}\frac{x(\log\log x)^k}{\log x}$$

结论对于$k+1$时也成立，故当$k\geqslant 2$时，

$$\pi_k(x)\sim\frac{1}{(k-1)!}\frac{x(\log\log x)^{k-1}}{\log x}.$$

因$p_1\cdots p_k$有$k!$种取法，上式乘以$k!$即得

$$\prod_k(x)\sim\frac{kx(\log\log x)^{k-1}}{\log x}\tag{5}$$

把（5）式代入（2）和（3）即得（9）

以上两种证明均由柯召教授给出。

§8 Dirichlet定理

习题 若 $(k,l)=1$，$l\leqslant k$，试证

$$\lim_{x\to\infty}\frac{\pi(x;k,l)}{\dfrac{x}{\varphi(k)\log x}}=1.$$

证： 此题的证明与素数定理的初等证明是相同的。

1）命 $\theta(x)=\sum\limits_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\log p$，$\psi(x)=\sum\limits_{\substack{n\leqslant x\\ n\equiv l(\bmod k)}}\Lambda(n)$

显然

$$\psi_l(x) = \theta_l(x) + \theta_l(x^{\frac{1}{2}}) + \theta_l(x^{\frac{1}{3}}) + \cdots$$

$$\psi_l(x) = \sum_{\substack{p\leqslant x \\ p\equiv l(\mathrm{mod}k)}} \left[\frac{\log x}{\log p}\right]\log p$$

因此 $\theta_l(x)\leqslant\psi_l(x)\leqslant\sum_{\substack{p\leqslant x \\ p\equiv l(\mathrm{mod}k)}} \frac{\log x}{\log p}\log p = \pi(x;\ k,\ l)\log x$

$$\overline{\lim_{x\to\infty}}\frac{\theta(x)}{x}\leqslant\overline{\lim_{x\to\infty}}\frac{\psi(x)}{x}\leqslant\overline{\lim_{x\to\infty}}\frac{\pi(x;k,l)}{x(\log x)^{-1}} \tag{1}$$

又设 $0<\alpha<1$，$x>1$，则

$$\theta(x)\geqslant\sum_{\substack{x^{\alpha}<p\leqslant x \\ p\equiv l(\mathrm{mod}k)}}\left\{\pi(x;k,l)-\pi(x^{\alpha};k,l)\right\}\log x^{\alpha}$$

$$\geqslant\alpha\left\{\pi(x;\ k,\ l)-x^{\alpha}\right\}\log x$$

因为 $\lim_{x\to\infty}\frac{\log x}{x^{1-\alpha}}=0$，故

$$\overline{\lim_{x\to\infty}}\frac{\theta(x)}{x}\geqslant\alpha\ \overline{\lim_{x\to\infty}}\frac{\pi(x;\ k,\ l)}{x(\log x)^{-1}}$$

对于任何小于 1 的正数α成立，故得

$$\overline{\lim_{x\to\infty}}\frac{\theta(x)}{x}\geqslant\overline{\lim_{x\to\infty}}\frac{\pi(x;\ k,\ l)}{x(\log x)^{-1}} \tag{2}$$

由（1）、（2）得

$$\overline{\lim_{x\to\infty}}\frac{\pi(x;\ k,\ l)}{x(\log x)^{-1}}=\overline{\lim_{x\to\infty}}\frac{\theta_l(x)}{x}=\overline{\lim_{x\to\infty}}\frac{\psi(x)}{x}$$

同理可得

$$\underline{\lim_{x\to\infty}}\frac{\pi(x;\ k,\ l)}{x(\log x)^{-1}}=\underline{\lim_{x\to\infty}}\frac{\theta_l(x)}{x}=\underline{\lim_{x\to\infty}}\frac{\psi(x)}{x}$$

上面两式可以写成

$$\overline{\lim_{x\to\infty}}\frac{\pi(x;\ k,\ l)}{\dfrac{x}{\varphi(k)\log x}}=\overline{\lim_{x\to\infty}}\frac{\theta_l(x)}{\dfrac{x}{\varphi(k)}}=\overline{\lim_{x\to\infty}}\frac{\psi_l(x)}{\dfrac{x}{\varphi(k)}}$$

$$\underline{\lim_{x\to\infty}}\frac{\pi(x;\ k,\ l)}{\dfrac{x}{\varphi(k)\log x}}=\underline{\lim_{x\to\infty}}\frac{\theta_l(x)}{\dfrac{x}{\varphi(k)}}=\underline{\lim_{x\to\infty}}\frac{\psi_l(x)}{\dfrac{x}{\varphi(k)}}$$

因此，如能证明

$$\theta_l(x)\sim\frac{x}{\varphi(k)}\text{ 或 }\psi_l(x)\sim\frac{x}{\varphi(k)},$$

即 $$\lim_{x\to\infty}\frac{\theta_l(x)}{\dfrac{x}{\varphi(k)}}=1\text{ 或 }\lim_{x\to\infty}\frac{\psi_l(x)}{\dfrac{x}{\varphi(k)}}=1,$$

那么，由熟知的关于极限存在的充分必要条件可得

$$\overline{\lim_{x\to\infty}}\frac{\pi(x;\ k,\ l)}{\dfrac{x}{\varphi(k)\log x}}=\underline{\lim_{x\to\infty}}\frac{\pi(x;\ k,\ l)}{\dfrac{x}{\varphi(k)\log x}}=1$$

即 $$\lim_{x\to\infty}\frac{\pi(x;\ k,\ l)}{\dfrac{x}{\varphi(k)\log x}}=1.$$

2）下面将证明两个不等式（3）和（4），它们在本题证明中所起的作用，与Selderg不等式在素数定理初等证明中所起的作用相同。

$$\sum_{\substack{p\leqslant x\\ p\equiv l(\mathrm{mod}k)}}\log^2 p+\sum_{\substack{pq\leqslant x\\ pq\equiv l(\mathrm{mod}k)}}\log p\log q=\frac{2}{\varphi(k)}x\log x+O(x)\qquad(3)$$

$$\theta_l(x)\log x+\sum_{p\leqslant x}\log p\,\theta_{l_p}\left(\frac{x}{p}\right)=\frac{2}{\varphi(k)}x\log x+O(x)\qquad(4)$$

这里$\bar{p}$为同余式 $p\bar{p}\equiv 1 \pmod{k}$ 的解．首先证明两个引理．

引理 1　当$h>0$时，

$$\sum_{n\leqslant x}\log^h\frac{x}{n}=O(x).$$

因为当$n\geqslant 2$时，

$$\log^h\frac{x}{n}\leqslant\int_{n-1}^{n}\log^h\frac{x}{t}dt,$$

从而
$$\sum_{n=2}^{[x]}\log^h\frac{x}{n}\leqslant\int_1^x\log^h\frac{x}{t}dt=x\int_1^x\frac{\log^h u}{u^2}du$$

$$<x\int_1^{\infty}\frac{\log^h u}{u^2}du=Ax,$$

此即
$$\sum_{n\leqslant x}\log^h\frac{x}{n}=O(x).$$

引理 2

$$\sum_{\substack{n\leqslant x\\ n\equiv l\pmod{k}}}\Lambda(n)\log n=\sum_{\substack{p\leqslant x\\ p\equiv l\pmod{k}}}\log^2 p+O(x)\tag{5}$$

$$\sum_{\substack{mn\leqslant x\\ mn\equiv l\pmod{k}}}\Lambda(m)\Lambda(n)=\sum_{\substack{pq\leqslant x\\ pq\equiv l\pmod{k}}}\log p\log q+O(x)\tag{6}$$

以及
$$\sum_{n\leqslant x}\Lambda(n)\log n=\sum_{p\leqslant x}\log^2 p+O(x)\tag{5'}$$

$$\sum_{mn\leqslant x}\Lambda(m)\Lambda(n)=\sum_{pq\leqslant x}\log p\log q+O(x)\tag{6'}$$

因为
$$\sum_{\substack{n\leqslant x\\ n\equiv l\pmod{k}}}\Lambda(n)\log n=\sum_{\substack{p^m\leqslant x\\ p^m\equiv l\pmod{k}\\ 1\leqslant m\leqslant\left[\frac{\log x}{\log 2}\right]}}m\log^2 p$$

$$=\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\log^2 p+\sum_{\substack{p^m\leqslant x\\ p^m\equiv l(\bmod k)\\ 2\leqslant m\leqslant\left[\frac{\log x}{\log 2}\right]}} m\log^2 p$$

$$=\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\log^2 p+O\left(\sum_{\substack{p^m\leqslant x\\ p^m\equiv l(\bmod k)\\ 2\leqslant m\leqslant\left[\frac{\log x}{\log 2}\right]}}\frac{\log x}{\log p}\log^2 p\right)$$

$$=\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\log^2 p+O\left(\log x\sum_{\substack{p^m\leqslant x\\ 2\leqslant m\leqslant\left[\frac{\log x}{\log 2}\right]}}\log p\right)$$

且

$$\sum_{\substack{p^m\leqslant x\\ 2\leqslant m\leqslant\left[\frac{\log x}{\log 2}\right]}}\log p=\theta(x^{\frac{1}{2}})+\theta(x^{\frac{1}{3}})+\cdots$$

$$\cdots+\theta\left(x^{1/\left[\frac{\log x}{\log 2}\right]}\right)=O(\log x\,\theta(x^{\frac{1}{2}}))=O(x^{\frac{1}{2}}\log x)$$

所以

$$\sum_{\substack{n\leqslant x\\ n\equiv l(\bmod k)}}\Lambda(n)\log n=\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\log^2 p+O(x).$$

此即（5）得证。又因为

$$\sum_{\substack{mn\leqslant x\\ mn\equiv l(\bmod k)}}\Lambda(m)\Lambda(n)=\sum_{\substack{p^\alpha q^\beta\leqslant x\\ p^\alpha q^\beta\equiv l(\bmod k)\\ \alpha\geqslant 1,\beta\geqslant 1}}\log p\log q$$

$$=\sum_{\substack{pq\leqslant x\\ pq\equiv l(\bmod k)}}\log p\log q+O\left(\sum_{\substack{p^\alpha\leqslant x\\ \alpha\geqslant 2}}\log p\sum_{\substack{q^\beta\leqslant x/p^\alpha\\ \beta\geqslant 1}}\log q\right)$$

$$= \sum_{\substack{pq\leqslant x\\ pq\equiv l\,(\mathrm{mod}k)}} \log p\log q + O\left(\sum_{\substack{p^a\leqslant x\\ a\geqslant 2}} \log p\psi\left(\frac{x}{p^a}\right)\right)$$

$$= \sum_{\substack{pq\leqslant x\\ pq\equiv l\,(\mathrm{mod}k)}} \log p\log q + O\left(x\sum_{p\leqslant\sqrt{x}}\sum_{a\geqslant 2}\frac{\log p}{p^a}\right)$$

$$= \sum_{\substack{pq\leqslant x\\ pq\equiv l\,(\mathrm{mod}k)}} \log p\log q + O\left(x\sum_{p\leqslant\sqrt{x}}\frac{\log p}{p(p-1)}\right)$$

$$= \sum_{\substack{pq\leqslant x\\ pq\equiv l\,(\mathrm{mod}k)}} \log p\log q + O(x)$$

此即 $$\sum_{\substack{mn\leqslant x\\ mn\equiv l\,(\mathrm{mod}k)}} \Lambda(m)\Lambda(n) = \sum_{\substack{pq\leqslant x\\ pq\equiv l\,(\mathrm{mod}k)}} \log p\log q + O(x)$$

从而（6）得证，用完全相同的方法可证(5′)、(6′)．这样就证明了引理2．设

$$S(x) = \sum_{n\leqslant x}\sum_{d\mid n}\mu(d)\log^2\frac{x}{d}$$

$$S_l(x) = \sum_{\substack{n\leqslant x\\ n\equiv l\,(\mathrm{mod}k)}}\sum_{d\mid n}\mu(d)\log^2\frac{x}{d}$$

从以下熟知的结果

$$\sum_{d\mid n}\mu(d) = 1,\ (n=1);\quad \sum_{d\mid n}\mu(d) = 0,\ (n>1).$$

$$\Lambda(n) = -\sum_{d\mid n}\mu(d)\log d;\quad \log n = \sum_{d\mid n}\Lambda(d)$$

可得 $$\sum_{h\mid n}\Lambda(h)\Lambda\left(\frac{n}{h}\right)=-\sum_{h\mid n}\Lambda(h)\sum_{d\mid \frac{n}{h}}\mu(d)\log d$$

$$=-\sum_{d\mid n}\mu(d)\log d\sum_{h\mid \frac{n}{d}}\Lambda(h)$$

$$=-\sum_{d\mid n}\mu(d)\log d\log\frac{n}{d}$$

$$=\Lambda(n)\log n+\sum_{d\mid n}\mu(d)\log^2 d$$

和 $\sum_{d\mid 1}\mu(d)\log^2\frac{x}{d}=\log^2 x$，从而当$n>1$时，

$$\sum_{d\mid n}\mu(d)\log^2\frac{x}{d}=\sum_{d\mid n}\mu(d)(\log^2 d-2\log x\log d)$$

$$=2\Lambda(n)\log x-\Lambda(n)\log n+\sum_{hr=n}\Lambda(h)\Lambda(r)$$

故 $$S_l(x)=\delta\log^2 x+2\psi_l(x)\log x-\sum_{\substack{n\leqslant x\\ n\equiv l(\bmod k)}}\Lambda(n)\log n$$

$$+\sum_{\substack{hr\leqslant x\\ hr\equiv l(\bmod k)}}\Lambda(h)\Lambda(r)$$

其中

$$\delta=\begin{cases}1, & \text{当}l\equiv 1(\bmod k)\text{时}\\ 0, & \text{当}\not\equiv 1(\bmod k)\text{时}\end{cases}$$

再在熟知的Abel变换中取

$$C_n=\begin{cases}\Lambda(n), & \text{当}n\equiv l(\bmod k)\text{时}\\ 0, & \text{当}n\not\equiv l(\bmod k)\text{时}\end{cases}$$

$C(t)=\sum_{n\leqslant t} C_n$， $f(t)=\log t$， 则有

$$\sum_{\substack{n\leqslant x\\ n\equiv l(\bmod k)}} \Lambda(n)\log n = \sum_{n\leqslant x} C_n f(n)$$

$$= C(x)f(x) = \int_2^x C(t)f'(t)dt$$

$$\psi_l(x)\log x - \int_2^x \frac{\psi(t)}{t}dt = \psi_l(x)\log x + O(x),$$

所以 $S_l(x)=\delta\log^2 x+2\psi_l(x)\log x-\sum\limits_{\substack{n\leqslant x\\ n\equiv l(\bmod k)}}\Lambda(n)\log n$

$$+\sum_{\substack{hr\leqslant x\\ hr\equiv l(\bmod k)}}\Lambda(h)\Lambda(r)$$

$$=\sum_{\substack{n\leqslant x\\ n\equiv l(\bmod k)}}\Lambda(n)\log n+\sum_{\substack{mn\leqslant x\\ mn\equiv l(\bmod k)}}\Lambda(m)\Lambda(n)+O(x)$$

再由引理 2 中的（5）、（6）立得

$$S_l(x)=\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\log^2 p+\sum_{\substack{pq\leqslant x\\ pq\equiv l(\bmod k)}}\log p\log+O(x) \qquad (7)$$

利用类似的方法并结合引理 2 中的(5′)、(6′)以及Selberg不等式可得

$$S(x)=\log^2 x+2\psi(x)\log x-\sum_{n\leqslant x}\Lambda(n)\log n+\sum_{hr\leqslant x}\Lambda(h)\Lambda(r)$$

$$=\sum_{n\leqslant x}\Lambda(n)\log n+\sum_{mn\leqslant x}\Lambda(m)\Lambda(n)+O(x)$$

$$=\sum_{p\leqslant x}\log^2 p+\sum_{pq\leqslant x}\log p\log q+O(x)$$

$$= 2x\log x + O(x) \tag{8}$$

由习题7．2．2可得

$$\varphi(k)S_l(x) = \varphi(k)\sum_{\substack{n\leqslant x\\ n\equiv l(\bmod k)}}\sum_{d\mid n}\mu(d)\log^2\frac{x}{d}$$

$$= \sum_{\chi}\bar{\chi}(l)\sum_{n\leqslant x}\chi(n)\sum_{d\mid n}\mu(d)\log^2\frac{x}{d}$$

$$= \sum_{\substack{n\leqslant x\\ (n,\ k)=1}}\sum_{d\mid n}\mu(d)\log^2\frac{x}{d} + \sum_{\substack{\chi\\ \chi\neq\chi_0}}\bar{\chi}(l)\sum_{n\leqslant x}\chi(n)$$

$$\sum_{d\mid n}\mu(d)\log^2\frac{x}{d} \tag{9}$$

由引理 1 和习题7.2.1可得

$$\sum_{n\leqslant x}\chi(n)\sum_{d\mid n}\mu(d)\log^2\frac{x}{d}$$

$$= \sum_{dd'\leqslant x}\chi(d')\chi(d)\mu(d)\log^2\frac{x}{d}$$

$$= \sum_{d\leqslant x}\chi(d)\mu(d)\log^2\frac{x}{d}\sum_{d'\leqslant\frac{x}{d}}\chi(d')$$

$$= O\left(\frac{\varphi(k)}{2}\sum_{d\leqslant x}\log^2\frac{x}{d}\right)$$

$$= O(x)$$

因此 $\sum_{\substack{\chi\\ \chi\neq\chi_0}}\bar{\chi}(l)\sum_{n\leqslant x}\chi(n)\sum_{d\mid n}\mu(d)\log^2\frac{x}{d} = O(x)$

故从（9）

$$\varphi(k)S_l(x) = \sum_{\substack{n\leqslant x\\ (n,\ k)=1}}\sum_{d\mid n}\mu(d)\log^2\frac{x}{d} + O(x) \tag{10}$$

如设l，l_2，…，$l_{\varphi(k)}$表k的缩系，则用完全相同的方法可得

$$\varphi(k)S_{l_i}(x)=\sum_{\substack{n\leqslant x\\(n,k)=1}}\sum_{d\mid n}\mu(d)\log^2\frac{x}{d}+O(x)$$

其中i满足条件$2\leqslant i\leqslant\varphi(k)$。将此$\varphi(k)$个式子相加得

$$S(x)+\sum_{i=2}^{\varphi(k)}S_{l_i}(x)=\sum_{\substack{n\leqslant x\\(n,k)=1}}\sum_{d\mid n}\mu(d)\log^2\frac{x}{d}+O(x)\qquad(11)$$

注意到

$$S(x)=S_l(x)+\sum_{i=2}^{\varphi(k)}S_{l_i}(x)+\sum_{n\leqslant k}\sum_{d\mid n}\mu(d)\log^2\frac{x}{d}+O(x)$$

从而（11）给出

$$S(x)=\sum_{\substack{n\leqslant x\\(n,k)=1}}\sum_{d\mid n}\mu(d)\log^2\frac{x}{d}+\sum_{n\leqslant k}\sum_{d\mid n}\mu(d)$$

$$\log^2\frac{x}{d}+O(x)$$

$$=\sum_{\substack{n\leqslant x\\(n,k)=1}}\sum_{d\mid n}\mu(d)\log^2\frac{x}{d}+O(x)$$

再由（7）、（8）、(10)得

$$S_l(x)=\frac{1}{\varphi(k)}S(x)+O(x)$$

即 $$\sum_{\substack{p\leqslant x\\p\equiv l(\mathrm{mod}k)}}\log^2p+\sum_{\substack{pq\leqslant x\\pq\equiv l(\mathrm{mod}k)}}\log p\log q=$$

$$=\frac{2}{\varphi(k)}x\log x+O(x)$$

这就证明了（3）式．另外，因为

$$\theta_l(x)\log x-\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\log^2 p=\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\log p\log\frac{x}{p}$$

$$=\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\log p\left(\sum_{n\leqslant\frac{x}{p}}\frac{1}{n}+O(1)\right)$$

$$=\sum_{n\leqslant x}\frac{1}{n}\sum_{\substack{p\leqslant\frac{x}{n}\\ p\equiv l(\bmod k)}}\log p+O(\theta_l(x))$$

$$=O\left(x\sum_{n\leqslant x}\frac{1}{n^2}\right)+O(x)=O(x)$$

即 $$\theta_l(x)\log x=\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\log^2 p+O(x) \qquad (12)$$

和 $$\sum_{p\leqslant x}\log p\theta_{\bar{p}}\left(\frac{x}{p}\right)=\sum_{\substack{pq\leqslant x\\ pq\equiv l(\bmod k)}}\log p\log q \qquad (13)$$

故只要把（12、（13）代入（3）便可得到（4）．

3）再证明7个）引理，这7个引理与素数定理初等证明过程中所使用的7个引理所起作用是相同的．命

$$R_l(x)=\theta_l(x)-\frac{x}{\varphi(k)}$$

由1）所述可知本习题结论与

$$\lim_{x\to\infty}\frac{R_l(x)}{x}=0$$

是等价的．

引理 1′　若$x\geqslant 3$，则

$$\sum_{pq\leqslant x}\frac{\log p\log q}{pq}=\frac{1}{2}\log^2 x+O(\log x),$$

$$\sum_{pq\leqslant x}\frac{\log p\log q}{pq\log pq}=\log x+O(\log\log x),$$

$$\sum_{p\leqslant x}\frac{\log p}{p\log\frac{2x}{p}}=O(\log\log x).$$

证：此即素数定理初等证明中的引理 1 .

引理 2′　若$x\geqslant 2$，则

$$\theta_l(x)+\sum_{\substack{pq\leqslant x\\ pq\equiv l(\mathrm{mod}k)}}\frac{\log p\log q}{\log pq}=\frac{2}{\varphi(k)}x+O\left(\frac{x}{\log x}\right).$$

证：设

$$B(n)=\sum_{\substack{pq\leqslant n\\ pq\equiv l(\mathrm{mod}k)}}\log p\log q,\quad C(n)=\sum_{\substack{p\leqslant n\\ p\equiv l(\mathrm{mod}k)}}\log^2 p$$

则由（3）、（4）得

$$\theta_l(x)+\sum_{\substack{pq\leqslant x\\ pq\equiv l(\mathrm{mod}k)}}\frac{\log p\log q}{\log pq}=\sum_{n\leqslant x}\frac{C(n)-C(n-1)}{\log n}$$

$$+\sum_{n\leqslant x}\frac{B(n)-B(n-1)}{\log n}$$

$$=\frac{C([x])}{\log[x]}+\frac{B([x])}{\log[x]}+\sum_{n\leqslant x-1}\left\{C(n)+B(n)\right\}$$

$$\left\{\frac{1}{\log n}-\frac{1}{\log(n+1)}\right\}$$

$$=\frac{2}{\varphi(k)}x+O\left(\frac{x}{\log x}\right)+\sum_{n\leqslant x-1}\left(\frac{2}{\varphi(k)}n\log n+O(n)\right)$$

$$\frac{\log\left(1+\frac{1}{n}\right)}{\log n\log(n+1)}$$

$$=\frac{2}{\varphi(k)}x+O\left(\frac{x}{\log x}\right)$$

引理3′　若$x\geqslant 3$，则

$$R_l(x)\log x=\sum_{pq\leqslant x}\frac{\log p\log q}{\log pq}R_{l\bar{p}\bar{q}}\left(\frac{x}{pq}\right)+O(x\log\log x)$$

证：当$x\geqslant 2$时，$\frac{x}{\log x}\leqslant\frac{2x}{\log 2x}$，故由引理2′有

$$\theta_l(x)+\sum_{\substack{pq\leqslant x\\ pq\equiv l(\bmod k)}}\frac{\log p\log q}{\log pq}=\frac{2}{\varphi(k)}x+O\left(\frac{x}{\log 2x}\right)$$

由上式和引理1′有

$$\sum_{p\leqslant x}\log p\,\theta_{l\bar{p}}\left(\frac{x}{p}\right)=\sum_{p\leqslant x}\log p\left(\frac{2}{\varphi(k)}\cdot\frac{x}{p}\right.$$

$$\left.-\sum_{\substack{qr\leqslant x/p\\ qr\equiv l\bar{p}(\bmod k)}}\frac{\log q\log r}{\log qr}+O\left(\frac{x/p}{\log 2x/p}\right)\right)$$

$$=\frac{2}{\varphi(k)}x\sum_{p\leqslant x}\frac{\log p}{p}-\sum_{p\leqslant x}\log p\sum_{\substack{qr\leqslant x/p\\ qr\equiv l\bar{p}(\bmod k)}}\frac{\log q\log r}{\log qr}$$

$$+O\left(x\sum_{p\leqslant x}\frac{\log p}{p\log 2x/p}\right)$$

$$=\frac{2}{\varphi(k)}x\log x-\sum_{qr\leqslant x}\frac{\log q\log r}{\log qr}\sum_{\substack{p\leqslant x/qr\\ p\equiv l\overline{qr}(\bmod k)}}\log p+$$

$$+O(x\log\log x)$$

$$=\frac{2}{\varphi(k)}x\log x-\sum_{qr\leqslant x}\frac{\log q\log r}{\log qr}\theta_{l\overline{qr}}\left(\frac{x}{p}\right)+O(x\log\log x)$$

再由（4）有

$$\theta_l(x)\log x=\frac{2}{\varphi(k)}x\log x-\sum_{p\leqslant x}\log p\,\theta_{l\bar{p}}\left(\frac{x}{p}\right)+O(x)$$

$$=\frac{2}{\varphi(k)}x\log x-\left(\frac{2}{\varphi(k)}x\log x-\sum_{qr\leqslant x}\frac{\log q\log r}{\log qr}\theta_{l\overline{qr}}\left(\frac{x}{qr}\right)\right.$$

$$\left.+O(x\log\log x)\right)+O(x)$$

$$=\sum_{qr\leqslant x}\frac{\log q\log r}{\log qr}\theta_{l\overline{qr}}\left(\frac{x}{qr}\right)+O(x\log\log x)\ ;$$

又因为 $\theta_l(x)=\dfrac{x}{\varphi(k)}+R_l(x)$

所以由引理 1′得

$$\theta_l(x)\log x=\sum_{qr\leqslant x}\frac{\log q\log r}{\log qr}\theta_{l\overline{qr}}\left(\frac{x}{qr}\right)-\frac{1}{\varphi(k)}x\log x$$

$$+O(x\log\log x)$$

$$=\sum_{qr\leqslant x}\frac{\log q\log r}{\log qr}\left(R_{l\overline{qr}}\left(\frac{x}{qr}\right)+\frac{1}{\varphi(k)}\cdot\frac{x}{qr}\right)$$

$$-\frac{1}{\varphi(k)}x\log x+O(x\log\log x)$$

$$=\sum_{qr\leqslant x}\frac{\log q\log r}{\log qr}R_{l\overline{qr}}\left(\frac{x}{qr}\right)+\frac{x}{\varphi(k)}\sum_{qr\leqslant x}\frac{\log q\log r}{qr\log qr}$$

$$-\frac{1}{\varphi(k)}x\log x+O(x\log\log x)$$

$$=\sum_{qr\leqslant x}\frac{\log q\log r}{\log qr}R_{l\overline{qr}}\left(\frac{x}{qr}\right)+\frac{x}{\varphi(k)}\left(\log x+O(\log\log x)\right)$$

$$-\frac{1}{\varphi(k)}x\log x+O(x\log\log x)$$

$$=\sum_{qr\leqslant x}\frac{\log q\log r}{\log qr}R_{l\overline{qr}}\left(\frac{x}{qr}\right)+O(x\log\log x)$$

$$=\sum_{pq\leqslant x}\frac{\log p\log q}{\log pq}R_{l\overline{pq}}\left(\frac{x}{pq}\right)+O(x\log\log x).$$

引理 4　若$x\geqslant3$，则

$$|R_l(x)|\leqslant\frac{1}{\varphi(k)\log x}\sum_{\substack{1\leqslant a\leqslant k\\(a,k)=1}}\sum_{n\leqslant x}\left|R_a\left(\frac{x}{n}\right)\right|$$

$$+O\left(\frac{x\log\log x}{\log x}\right).$$

证：应用引理3′，证法与素数定理初等证明中的引理 4 相同。

引理 5′　若$x\geqslant 2$，则

$$\sum_{n\leqslant x}\frac{\theta(n)}{n^2}=\frac{1}{\varphi(k)}\log x+O(1),$$

$$\sum_{n\leqslant x}\theta\left(\frac{x}{n}\right)=\frac{1}{\varphi(k)}x\log x+O(x).$$

证：证明方法与素数定理初等证明中的引理 5 相同，并利用定理 2 可证。

引理 6′　若$x\geqslant2$，则

$$\sum_{n\leqslant x}\frac{\log n}{n}R_l(n)=-\sum_{n\leqslant x}\frac{1}{n}\sum_{\alpha\beta\equiv l(\bmod k)}R_\alpha(n)R_\beta\left(\frac{x}{n}\right)+O(x).$$

证：应用引理5′，证法与引理6相同。

引理 7′　若$0<\sigma<1$，且存在x_0，当$x>x_0$时$|R_l(x)|<$

$\frac{\sigma x}{\varphi(k)}$，则必存在$x_\sigma$，当$x>x_\sigma$时，区间$((1-\sigma)^{16}x, x)$皆包含一个子区间$(y, e^\delta y)$，此处$\delta=\frac{\sigma(1-\sigma)}{32}$。当$y\leqslant z\leqslant e^\delta y$时

$$\left|\frac{R(z)}{z}\right|<\frac{1}{\varphi(k)}\frac{\sigma+\sigma^2}{2}.$$

证：应用引理6′，证法与引理7相同。

4）最后我们用定理2即估计式

$$\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\frac{\log p}{p}=\frac{1}{\varphi(k)}\log x+O(1) \tag{1}$$

来证明存在正数$c<1$。当$x>x_0$时，不等式

$$\theta(x)>\frac{c}{\varphi(k)}x$$

成立。(1)可写成

$$\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\frac{\log p}{p}=\frac{1}{\varphi(k)}\log x+A_l(x) \tag{1'}$$

其中$A_l(x)$满足$|A_l(x)|<\frac{M}{\varphi(k)}$，而$M$是某一个确定的正数。取正数$c<1$。如果$x\geqslant 1$，$cx\geqslant 1$，则由(1′)可得

$$\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\frac{\log p}{p}-\sum_{\substack{p\leqslant cx\\ p\equiv l(\bmod k)}}\frac{\log p}{p}$$

$$=\left(\frac{1}{\varphi(k)}\log x+A(x)\right)-\left(\frac{1}{\varphi(k)}\log cx+A(x)\right)$$

$$\geqslant-\frac{1}{\varphi(k)}\log c-|A_l(x)|-|A_l(cx)|$$

$$> -\frac{1}{\varphi(k)}\log c - \frac{2M}{\varphi(k)}$$

取$c = e^{-(2M+1)}$，则上式给出

$$\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\frac{\log p}{p} - \sum_{\substack{p\leqslant cx\\ p\equiv l(\bmod k)}}\frac{\log p}{p} > \frac{1}{\varphi(k)}，当\ x \geqslant \frac{1}{c}时.$$

另一方面，又因为

$$\sum_{\substack{p\leqslant x\\ p\equiv l(\bmod k)}}\frac{\log p}{p} - \sum_{\substack{p\leqslant cx\\ p\equiv l(\bmod k)}}\frac{\log p}{p}$$

$$= \sum_{\substack{cx\leqslant p\leqslant x\\ p\equiv l(\bmod k)}}\frac{\log p}{p} < \frac{1}{cx}\sum_{\substack{p\leqslant x\\ p\leqslant l(\bmod k)}}\log p = \frac{1}{cx}\theta_l(x),$$

故若取$x_0 = \frac{1}{c}$，则有

$$\theta_l(x) > \frac{c}{\varphi(k)}x，当 x > x_0 时.$$

由不等式(4)有

$$\theta_l(x) = \frac{2}{\varphi(k)}x - \frac{1}{\log x}\sum_{p\leqslant x}\theta_{lp}\left(\frac{x}{p}\right)\log p + O\left(\frac{x}{\log x}\right)$$

$$= \frac{2}{\varphi(k)}x - \frac{1}{\log x}\sum_{p\leqslant \frac{x}{x_0}}\theta_{lp}\left(\frac{x}{p}\right)\log p - \frac{1}{\log x}\sum_{\frac{x}{x_0}<p\leqslant x}$$

$$\theta_{lp}\left(\frac{x}{p}\right)\log p + O\left(\frac{x}{\log x}\right)$$

$$\leqslant \frac{2}{\varphi(k)}x - \frac{c}{\varphi(k)}x\cdot\frac{\log x}{\log x} + O\left(\frac{1}{\log x}\sum_{\frac{x}{x_0}\leqslant p\leqslant x}\log p\right)$$

$$+O\left(\frac{x}{\log x}\right)$$

$$=\frac{2-c}{\varphi(k)}x+O\left(\frac{x}{\log x}\right)<\frac{1}{\varphi(k)}\left(2-\frac{c}{2}\right)x$$

再据$R_l(x)=\theta_l(x)-\frac{1}{\varphi(k)}x$可得

$$\left|R_l(x)\right|<\frac{1}{\varphi(k)}\sigma_0 x \quad (x>x_0,\quad \sigma_0=\left|1-\frac{c}{2}\right|,$$

$$0<\sigma_0<1).$$

命

$$\zeta=(1-\sigma_0)^{-16} \qquad \delta=\frac{\sigma_0(1-\sigma_0)}{32}$$

由引理7′知存在$x_{\sigma_0}>x_0$，当$x>x_{\sigma_0}$时，任何区间$(\nu-1,\ \zeta\nu)$，$\left(\zeta\leqslant\zeta\nu\leqslant\frac{x}{x_{\sigma_0}}\right)$都包有子区间$(y_\nu,\ e^{\delta}y_\nu)$当$y_\nu\leqslant n\leqslant e^{\delta}y_\nu$时，

$$\left|\frac{n}{x}R_l\left(\frac{x}{n}\right)\right|<\frac{1}{\varphi(k)}\cdot\frac{\sigma_0+\sigma_0{}^2}{2}.$$

由引理4′可知

$$\left|R_l(x)\right|<\frac{1}{\varphi(k)\log x}\sum_{\substack{1\leqslant a\leqslant k\\(a,\ k)=1}}\ \sum_{n\leqslant\frac{x}{x_{\sigma_0}}}\left|R_a\left(\frac{x}{n}\right)\right|$$

$$+\frac{1}{\varphi(k)\log x}\sum_{\substack{1\leqslant a\leqslant k\\(a,\ k)=1}}\ \sum_{\frac{x}{x_{\sigma_0}}<n\leqslant x}\left|R_a\left(\frac{x}{n}\right)\right|$$

$$+O\left(\frac{x}{\sqrt{\log x}}\right)$$

$$<\frac{\sigma_0 x}{\varphi(k)\log x}\sum_{\substack{1\leqslant n\leqslant \frac{x}{x_{\sigma_0}}\\ n\in(y_\nu,\ e^\delta y_\nu)}}\frac{1}{n}+\frac{\sigma_0+\sigma_0{}^2}{2\varphi(k)}\cdot\frac{x}{\log x}\sum_{\zeta^\nu\leqslant\frac{x}{x_{\sigma_0}}}$$

$$\sum_{y_\nu\leqslant n\leqslant e^\delta y_\nu}\frac{1}{n}+O\left(\frac{x}{\sqrt{\log x}}\right)$$

$$<\frac{\sigma_0 x}{\varphi(k)\log x}\sum_{n\leqslant\frac{x}{x_{\sigma_0}}}\frac{1}{n}-\frac{\sigma_0-\sigma_0{}^2}{2\varphi(k)}\cdot\frac{x}{\log x}\sum_{\zeta^v\leqslant\frac{x}{x\sigma_0}}$$

$$\sum_{y_\nu\leqslant n\leqslant e^\delta y_\nu}\frac{1}{n}+O\left(\frac{x}{\sqrt{\log x}}\right)$$

$$<\frac{\sigma_0 x}{\varphi(k)}-\frac{\sigma_0-\sigma_0{}^2}{2\varphi(k)}\cdot\frac{x}{\log x}\sum_{\zeta^v\leqslant\frac{x}{x\sigma_0}}\left(\delta+O\left(\frac{1}{\zeta^\nu}\right)\right)$$

$$+O\left(\frac{x}{\sqrt{\log x}}\right)$$

$$<\frac{\sigma_0 x}{\varphi(k)}-\frac{\sigma_0-\sigma_0{}^2}{2\,\varphi(k)}\cdot\frac{x}{\log x}\frac{\delta\log x}{\log}+O\left(\frac{x}{\sqrt{\log x}}\right)$$

$$<\frac{\sigma_0}{\varphi(k)}\left(1-\frac{(1-\sigma_0)^2\sigma_0}{1024\log\frac{1}{1-\sigma_0}}\right)x+O\left(\frac{x}{\sqrt{\log x}}\right)$$

$$<\frac{\sigma_0}{\varphi(k)}\left(1-\frac{(1-\sigma_0)^3}{1024}\right)x+O\left(\frac{x}{\sqrt{\log x}}\right)$$

$$<\frac{\sigma_0}{\varphi(k)}\left(1-\frac{(1-\sigma_0)^3}{2000}\right)x=\frac{\sigma_1}{\varphi(k)}x,\quad(x>x_{\sigma_1}>x_{\sigma_0})$$

此处$\sigma_1<\sigma_0$．不断用上面的手续得到

$$\left|\mathrm{R}_l(x)\right|<\frac{\sigma_n}{\varphi(k)}x,\quad(x>x_{\sigma_n})$$

此处

$$\sigma_n=\sigma_{n-1}\left(1-\frac{(1-\sigma_{n-1})^3}{2000}\right)\leqslant\sigma_{n-1}\left(1-\frac{(1-\sigma_0)^3}{2000}\right)$$

$$\leqslant\cdots\leqslant\sigma_0\left(1-\frac{(1-\sigma_0)^3}{2000}\right)^n$$

故

$$\lim_{n\to\infty}\sigma_n=0,\ \lim_{n\to\infty}\frac{\sigma_n}{\varphi(k)}=0,\ \text{lmi}_{n\to\infty}\frac{R(x)}{x}=0;$$

又因为 $\dfrac{\theta_l(x)}{x}=\dfrac{1}{\varphi(k)}+\dfrac{R(x)}{x}$

所以 $\lim\limits_{x\to\infty}\dfrac{\theta(x)}{x}=\lim\limits_{x\to\infty}\left(\dfrac{1}{\varphi(k)}+\dfrac{R(x)}{x}\right)=\dfrac{1}{\varphi(k)}$

即

$$\lim_{x\to\infty}\frac{\theta(x)}{\dfrac{x}{\varphi(k)}}=1,$$

由 1）得 $\lim\limits_{x\to\infty}\dfrac{\pi(x;k,l)}{\dfrac{x}{\varphi(k)\log x}}=1$

讨论：用l_1，…，$l_{\varphi(k)}$表k的缩系，此题表明

$\pi(x;\ k,\ l_1)$，…，$\pi(x;\ k,\ l_{\varphi(k)})$

是两两渐近相等的，即对任何$i\neq j$，都有$\pi(x,\ k,\ l_i)\sim\pi(x;\ k,l_j)$。这说明，不超过$x$的素数，在$\varphi(k)$个算术级数$l_i+nk$中是“平均”分配的。

第十章　渐近法与连分数

一、提　　要

定义　分数

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cdots+\cfrac{1}{a_N}}}}$$

称为有限连分数．若$N=\infty$，则简称连分数，通常以$a_0+\frac{1}{a_1}+\frac{1}{a_2}+\cdots+\frac{1}{a_N}$或〔$a_0$，$a_1$，…，$a_N$〕表示．

定义　〔a_0，a_1…，a_n〕$=\frac{p_n}{q_n}$，$0\leqslant n\leqslant N$，称为〔a_0，a_1，…，a_N〕的第n个渐近值或渐近分数．

定理 1　渐近值间有如下关系：

$p_0=a_0$，$p_1=a_1a_0+1$，$p_n=a_np_{n-1}+p_{n-2}$，

$q_0=1$，$q_1=a_1$，$q_n=a_n q_{n-1}+q_{n-2}$.

上面的n满足条件$2\leqslant n\leqslant N$。

定理 2　p_n及q_n满足下列各式

$$p_n q_{n-1}-p_{n-1}q_n=(-1)^{n-1},\quad (n\geqslant 1);$$

及

$$p_n q_{n-2}-p_{n-2}q_n=(-1)^n a_n,\quad (n\geqslant 2).$$

定义　如果a_0为整数，a_1，a_2，…，都是正整数，称则$a_0+\frac{1}{a_1}+\frac{1}{a_2}+\cdots$为简单连分数。

定理 3　凡有理数必可表为有限连分数。

定理 4　用简单连分数表无理数的表示法是唯一的。

定理 5　若α为无理数，则

$$\lim_{n\to\infty}\frac{p_n}{q_n}=\alpha.$$

定理 6　若α为无理数，则必有无穷多个$\frac{p}{q}$，使得

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{2q^2}$$

成立

定理 7　若α为无理数，则必有无穷多个渐近分数，使得

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{\sqrt{5}\,q^2}$$

成立。

定义　当$l\geqslant \mathrm{L}$时，若$a_l=a_{l+k}$，则称此连分数为以k为周期的循环连分数，写作

$$[a_0,\ \cdots,\ a_{\mathrm{L}-1},\dot{a}_{\mathrm{L}},\ \cdots,\dot{a}_{\mathrm{L}+k-1}].$$

定理 8　一连分数为循环连分数的充分必要条件是此数为一有有理系数的二次不可化方程的根。

定理 9　若有理数$\frac{p}{q}$适合

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{2q^2},$$

则$\frac{p}{q}$必为α的一个渐近值。

定理10 若$p>0$，$q>0$，且

$$|p^2-\alpha^2q^2|<\alpha,$$

则$\frac{p}{q}$必为α的一个渐近值。

定理11 不定方程

$$x^2-dy^2=l, \quad 0<|l|<\sqrt{d}$$

如果d是正整数且非平方数，则

$$a_n'=[a_n, a_{n+1}, \cdots]=\frac{\sqrt{d}+P_n}{Q_n},$$

$P_n^2\equiv d(\mathrm{mod} Q_n)$，$P_n$，$Q_n$都是整数。

定理12 二次不定方程

$$x^2-dy^2=l,$$

当$l=(-1)^nQ_n$时一定可解；当$l\neq(-1)^n$且$|l|<\sqrt{d}$时则一定不可解。

定理13 命n为使$(-1)^nQ_n=1$的最小正整数，则Pell方程

$$x^2-dy^2=1$$

的所有解由下式给出

$$x+\sqrt{d}\,y=\pm(p_{n-1}+\sqrt{d}\,q_{n-1})^l, \quad l\text{为整数。}$$

定理14 设θ为一无理数，β为任一的实数，则有无穷多对整数x，y，使

$$\left|\theta x-y-\beta\right|<\frac{3}{x}$$

成立。

定理15 设θ为一无理数，β为实数，对任给的$\varepsilon>0$，不等

式

$$\left|\theta x-y-\beta\right|<\frac{1+\varepsilon}{\sqrt{5}x}$$

有无穷多对整数解$x>0$，y。

定义 若$P_i(i=1, 2, \cdots)$为$(0, 1)$中的一点集，若对任一自然数n及合条件$0\leqslant a<b\leqslant 1$的任二数$a$，$b$，$P_1$，…，$P_n$，$n$个点中，其落入区间$(a, b)$中的数目$N_n(a, b)$满足关系

$$\lim_{n\to\infty}\frac{N_n(a, b)}{n}=b-a,$$

则称点集$P_i(i=(1, 2, \cdots)$在$(0, 1)$内一致分布。

定理16 若θ为一无理数，则点集

$$\{x\theta\}=x\theta-[x\theta],\ x=1, 2, \cdots$$

在$(0, 1)$中一致分布。

定理17 一数列

$$x_1, \cdots, x_m, \cdots \qquad 0\leqslant x_m\leqslant 1$$

是一致分布的充分必要条件为对任一$(0, 1)$区间Riemann可积函数$f(x)$常有

$$\lim_{n\to\infty}\frac{f(x_1)+\cdots+f(x_n)}{n}=\int_0^1 f(x)dx.$$

二、题　解

§1　简单连分数

习题1 求证

$$p_n=\begin{vmatrix} a_0 & -1 & 0 & 0\cdots 0 & 0 & 0 \\ 1 & a_1 & -1 & 0\cdots 0 & 0 & 0 \\ 0 & 1 & a_2 & -1\cdots 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0\cdots 1 & a_{n-1} & -1 \\ 0 & 0 & 0 & 0\cdots 0 & 1 & a_n \end{vmatrix}$$

并证明q_n为由上行列式中除去第一行第一列后之行列式之数值。

证： $n=0$时$p_0=a_0$，$n=1$时，

$$p_1=\begin{vmatrix} a_0 & -1 \\ 1 & a_1 \end{vmatrix}=a_0a_1+1.$$

归纳假定直到$n-1$时结论成立，即有

$$p_{n-1}=\begin{vmatrix} a_0 & -1 & & & \\ 1 & a_1 & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & 1 & a_{n-2} & -1 \\ & & & 1 & a_{n-1} \end{vmatrix}=a_{n-1}p_{n-2}+p_{n-3}.$$

把p_n所对应的行列式按最后一列展开有

$$p_n=a_n\begin{vmatrix} a_0 & -1 & & & \\ 1 & a_1 & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & 1 & a_{n-2} & -1 \\ & & & 1 & a_{n-1} \end{vmatrix}+\begin{vmatrix} a_0 & -1 & & & \\ 1 & a_1 & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & 1 & a_{n-2} & -1 \\ & & & 0 & 1 \end{vmatrix}.$$

由归纳假定，第一行列式的值为p_{n-2}。再把第二个行列式按最后一行展开 其值为p_{n-2}，故有$p_n=a_np_{n-1}+p_{n-2}$。下面再证明

$$q_n=\begin{vmatrix} a_1 & -1 & & & \\ 1 & a_2 & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & 1 & a_{n-1} & -1 \\ & & & 1 & a_n \end{vmatrix}$$

当$n=1$时，$q_1=a_1$。归纳假定直到$n-1$时结论成立，即有

$$q_{n-1}=\begin{vmatrix} a_1 & -1 & & & \\ 1 & a_2 & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & 1 & a_{n-2} & -1 \\ & & & 1 & a_{n-1} \end{vmatrix}$$

把q_n所对应的行列式按最后一列展开有

$$q_n=a_n\begin{vmatrix} a_1 & -1 & & & \\ 1 & a_2 & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & 1 & a_{n-2} & -1 \\ & & & 1 & a_{n-1} \end{vmatrix}+\begin{vmatrix} a_1 & -1 & & & \\ 1 & a_2 & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & 1 & a_{n-2} & -1 \\ & & & 0 & 1 \end{vmatrix}$$

由归纳假定，第一行列式的值为q_{n-1}。再把第二个行列式按最后一行展开，其值为q_{n-2}，故有$q_n=a_n q_{n-1}+q_{n-2}$。

习题 2 贯 $\{u_n\}$：

$$1, 1, 2, 3, 5, 8, 13, 21, \cdots$$

（$u_1=u_2=1$，$u_{i+1}=u_{i-1}+u_i$ （$i>1$））称之为Fibonacci贯．试证明

（i）$\frac{1}{2}\left(1+\sqrt{5}\right)$之第$n$个渐近分数为$\frac{u_{n+2}}{u_{n+1}}$；

（ii）若连分数$[a_0, a_1, \cdots, a_n, \cdots]$之诸$a_n$中除$a_i=2$（$i>0$）外，所有之$a_n$（$i\neq n$）皆等于1，则当$m>i$时有

$$\frac{p_m}{q_m}=\frac{u_{i+1}u_{m-i+3}+u_i u_{m-i+1}}{u_i u_{m-i+3}+u_{i-1}u_{m-i+1}}.$$

证：先证（i）．把$\frac{1}{2}\left(1+\sqrt{5}\right)$展成连分数：

$$\frac{1}{2}\left(1+\sqrt{5}\right)=[1, 1, \cdots].$$

设$\frac{p_n}{q_n}$为[1，1，…]的第n个渐近分数，下面用数学归纳法证明

$$p_n=u_{n+2}, \quad q_n=u_{n+1}.$$

$n=1$时，$p_1=2$，$q_1=1$，$u_3=2$，$u_2=1$，$\frac{p_1}{q_1}=\frac{u_3}{u_2}$。归纳假定$n\leqslant k$时结论成立，当$n=k+1$时，

$$p_{k+1}=a_{k+1}p_k+p_{k-1}=p_k+p_{k-1}=u_{k+2}+u_{k+1}\quad u_{k+3};$$

$$q_{k+1}=a_{k+1}q_k+q_{k-1}=q_k+q_{k-1}=u_{k+1}+u_k=u_{k+2}.$$

此即结论对于$n=k+1$时也成立。从而

$$p_n=u_{n+2}, \quad q_n=u_{n+1}$$

故$\frac{u_{n+2}}{u_{n+1}}$为$\frac{1}{2}\left(1+\sqrt{5}\right)$的第$n$个渐近分数。

再证（ii），此时必须假定$u_0=0$。下面用归纳法证明对任意的$m>i>0$，都有

$$p_m=u_{i+1}u_{m-i+3}+u_iu_{m-i+1}.$$

当$m=i+1$时，

$$p_m=p_{i+1}=a_{i+1}p_i+p_{i-1}=p_i+p_{i-1},$$

$$u_{i+1}u_{m-i+3}+u_iu_{m-i+1}=u_{i+1}u_4+u_iu_2=3u_{i+1}+u_i.$$

再用归纳法证明对任意的$i>0$，都有

$$p_i+p_{i-1}=3u_{i+1}+u_i$$

成立，从而当$m=i+1$时结论成立。$i=1$时

$$p_i+p_{i-1}=p_1+p_0=3+1=4$$

$$3u_{i+1}+u_i=3u_2+u_1=3\times1+1=4$$

即$i=1$时，$p_i+p_{i-1}=3u_{i+1}+u_i$。设$i=k$时等式等成立，即

$$p_k+p_{k-1}=3u_{k+1}+u_k$$

则当$i=k+1$时，

$$p_{k+1}+p_k=a_{k+1}p_k+p_{k-1}+p_k$$

$$=p_k+p_{k-1}+p_k=3u_{k+1}+u_k+p_k$$

$$=3u_{k+1}+u_k+p_{k-1}+p_{k-2}=3u_{k+1}+u_k+3u_k+u_{k-1}$$

$$=3(u_{k+1}+u_k)+u_k+u_{k-1}=3u_{k+2}+u_{k+1}$$

此即$i=k+1$时，

$$p_i+p_{i-1}=3u_{i+1}+u_i$$

也成立，故$m=i+1$时，

$$p_m=u_{i+1}u_{m-i+3}+u_iu_{m-i+1}$$

成立。

归纳假定对任意的$m=n>i+1$时，都有

$$p_m=u_{i+1}u_{m-i+3}+u_iu_{m-i+1},$$

那么当$m=n+1$时，

$$p_{n+1}=a_{n+1}p_n+p_{n-1}=p_n+p_{n-1}$$

$$=u_{i+1}u_{n-i+3}+u_iu_{n-i+1}+u_{i+1}u_{n-i+2}+u_iu_{n-i}$$

$$=u_{i+1}(u_{n-i+3}+u_{n-i+2})+u_i(u_{n-i+1}+u_{n-i})$$

$$=u_{i+1}u_{n-i+4}+u_iu_{n-i+2}$$

此即$p_m=u_{i+1}u_{m-i+3}+u_iu_{m-i+1}$在$m=n+1$时也成立。

故对任意的$i>0$，只要$m>i$，就有

$$p_m=u_{i+1}u_{m-i+3}+u_iu_{m-i+1}.$$

同理可证，对任意的$i>0$，只要$m>i$，就有

$$q_n=u_iu_{m-i+3}+u_{i-1}u_{m-i+1}.$$

所以对任意的$i>0$，只要$m>i$，就有

$$\frac{p_m}{q_m}=\frac{u_{i+1}u_{m-i+3}+u_iu_{m-i+1}}{u_iu_{m-i+3}+u_{i-1}u_{m-i+1}}.$$

习题 3 吾人知道，朔望月就是从太阳上来看月球绕地球一周所需的时间，也就是相同的月面位相间相隔的时间，它等于29.5306日；交点月，就是月球在它的轨道上从“交点”开始绕地球一周再回到这个“交点”所需的时间（所谓“交点”就月球绕地球轨道跟地球绕太阳轨道的交点）等于27.2123日.试证日、月蚀之周期为18年又11天*.

证：

$$\frac{29.5306}{27.2123}=〔1,\ 11,\ 1,\ 2,\ 1,\ 4,\ 2,\ 9,\ 1,\ 25,\ 2〕$$

因为$〔1,\ 11〕=\frac{12}{11}$

$$|11\times 29.5306-12\times 27.2123|=1.711$$

所以，如果把经过11个朔望月或12个交点月作为月蚀周期，误差为1.71天.

因为$〔1,\ 11,\ 1〕=\frac{13}{12}$

$$|12\times 29.5306-13\times 27.2123|=0.6073$$

所以如果把经过12个朔望月或13个交点月作为月蚀周期，误差为0.61天.

因为$〔1,\ 11,\ 1,\ 2〕=\frac{38}{35}$

$$|35\times 29.5306-38\times 27.2123|=0.4964$$

所以如果把经过35个朔望月或38个交点月作为月蚀周期，误差为0.50天. 因为$\left[1,\ 11,\ 1,\ 2,\ 1\right]=\frac{51}{47}$

$$|47\times 29.5306-51\times 27.2123|=0.1109$$

---

* 原题为18年零10天.

所以如果把经过47个朔望月或51个交点月作为月蚀周期，误差为0.11天。

因为〔1，11，1，2，14〕$=\frac{242}{223}$

$$|223\times29.5306-242\times27.2123|=0.0528$$

所以如果把经过223个朔望月或242个交点月作为月蚀周期，误差只有0.05天＝1.2小时。故可把经过223个朔望月或242个交点月作为月蚀周期，它等于

$$\begin{aligned}223\times29.5306\text{天}&=6585.3238\text{天}\\&\approx18\text{年零}11\text{天}.\end{aligned}$$

习题 4　火星最亮和离地球最近的一年，叫做火星的大冲．吾人知道，地球公转一周的周期是$365\frac{1}{4}$日，火星是687日．试证火星的大冲每隔15年一次．

证：

$$\frac{687}{365.25}=〔1,\ 1,\ 7,\ 2,\ 1,\ 1,\ 11〕$$

因为〔1，1〕$=\frac{2}{1}$

$$|2\times365.25-1\times678|=43.5$$

所以如果把经过2年作为火星大冲周期，误差为43.5天．

因为〔1，1，7〕$=\frac{15}{8}$

$$|15\times365.25-8\times687|=17.25$$

所以如果把15年作为火星大冲周期，误差只有半个月左右，故可把15年作为火星大冲周期．

§10 Чебышев定理及Хинчин定理

习题 试证明，若θ为一无理数，其对任一$\varepsilon>0$常有整数x及y，使

$$|x\theta-y|<\frac{\varepsilon}{x},$$

则对任一$\delta>0$及任一实数β，常有整数$x>0$及y，使

$$|x\theta-y-\beta|<\frac{1+\delta}{3x}.$$

证：首先证明对任给的$\varepsilon>0$，存在无穷多对整数p、q，$(p,q)=1$，使得

$$\theta=\frac{p}{q}+\frac{\varepsilon\delta_1}{q^2},\quad 0<|\delta_1|<\frac{1}{\sqrt{5}}$$

由题设知道存在整数对x_1、y_1，使得

$$|x_1\theta-y_1|<\frac{\varepsilon}{x_1}$$

对于$|x_1\theta-y_1|$，同样有整数对x_2、y_2，使得

$$|x_2\theta-y_2|<\frac{|x_1\theta-y_1|}{x_2}<\frac{\varepsilon}{x_2}$$

对于$|x_2\theta-y_2|$，也有整数对x_3、y_3，使得

$$|x_3\theta-y_3|<\frac{|x_2\theta-y_2|}{x_3}<\frac{\varepsilon}{x_3}$$

用上法可以得到

$$|x_1\theta-y_1|<\frac{\varepsilon}{x_1}$$

$$|x_2\theta-y_2|<\frac{\varepsilon}{x_2}$$

……

$$|x_m\theta-y_m|<\frac{\varepsilon}{x_m}$$

……

并且显然有

$$\cdots<|x_m\theta-y_m|<|x_{m-1}\theta-y_{m-1}|<\cdots<|x_2\theta-y_2|<|x_1\theta-y_1|$$

这就证明，对于任给的$\varepsilon>0$，存在无穷多个整数对x、y，使得

$$|x\theta-y|<\frac{\varepsilon}{x}$$

成立．设

$$|x_1\theta-y_1|=\frac{\varepsilon|\Delta_1|}{x_1},\quad 0<|\Delta_1|<1$$

因为x可任意大，故可假定$0<\frac{|\Delta_1|}{x_1}<\frac{1}{\sqrt{5}}$（只需要$x_1>\sqrt{5}$）．

那么由前述可得

$$|x_2\theta-y_2|=\frac{|x_1\theta-y_1||\Delta_2|}{x_2}=\frac{\varepsilon|\Delta_2||\Delta_1|}{x_2x_1}$$

$$|x_3\theta-y_3|=\frac{|x_2\theta-y_2||\Delta_3|}{x_3}=\frac{\varepsilon|\Delta_3||\Delta_2||\Delta_1|}{x_3x_2x_1}$$

……

$$|x_m\theta-y_m|=\frac{|x_{m-1}\theta-y_{m-1}||\Delta_m|}{x_m}$$

$$=\frac{\varepsilon|\Delta_m||\Delta_{m-1}|\cdots|\Delta_2||\Delta_1|}{x_mx_{m-1}\cdots x_2x_1}$$

其中$0<|\Delta_m|<1$，　$m=2$，3，……

因此如果令

$$\overline{\Delta}_m=\frac{|\Delta_m|\cdots|\Delta_1|}{x_{m-1}\cdots x_{\cdot}}$$

就得到 $|x_m\theta - y_m| = \dfrac{\varepsilon\overline{\Delta}_m}{x_m}$

再设$\theta = \dfrac{y_m}{x_m} + \dfrac{\varepsilon\delta_1}{x_m^2}$，则有

$$|\delta_1| = |\overline{\Delta}_m| = \overline{\Delta}_m$$

又因为显然有 $0 < \overline{\Delta}_m < \dfrac{1}{\sqrt{5}}$，做得

$$0 < |\delta_1| < \frac{1}{\sqrt{5}}$$

这便证明，对任给的$\varepsilon > 0$，存在无穷多个整数对p、q，$(p,q) = 1$，使得

$$\theta = \frac{p}{q} + \frac{\varepsilon\delta_1}{q^2},\quad 0 < |\delta_1| < \frac{1}{\sqrt{5}}$$

不妨设 $0 < \delta_1 < \dfrac{1}{\sqrt{5}}$，因为若有无穷多对整数$p$及$q$，$(p,q) = 1$，使得

$$\theta = \frac{p}{q} + \frac{\varepsilon\delta_1}{q^2},\quad -\frac{1}{\sqrt{5}} < \delta_1 < 0$$

只需设$\theta' = -\theta$，$p' = -p$，$\delta_1' = -\delta_1$，则对于θ'就有无穷多个整数对p'、q，$(p', q) = 1$，使得

$$\theta' = \frac{p'}{q} + \frac{\varepsilon\delta_1'}{q^2}$$

成立，并且满足条件

$$0 < \delta_1' < \frac{1}{\sqrt{5}}$$

此时，如能证明对任给的$\delta > 0$及实数$\beta' = -\beta$，常有整数$x > 0$及y'，使得

$$|x\theta'-y'-\beta'|<\frac{1+\delta}{3x}$$

成立，实际上也就证明了

$$|x\theta-y-\beta|<\frac{1+\delta}{3x}$$

是成立的。在上述不等式中，$y'=-y$。故常可以假定$0<\delta_1<\frac{1}{\sqrt{5}}$。

1）若ξ_1、ξ_2为任意二实数（后面确定），且$\xi_2-\xi_1\geqslant 1$，则常可求得整数对x、y，使得

$$px-qy=[q\beta],\quad \xi_1 q\leqslant x<\xi_2 q$$

因此 $|x\theta-y-\beta|=\frac{1}{q}\left|\frac{x\varepsilon\delta_1}{q}-\tau\right|=\frac{1}{x}\cdot\frac{x}{q}\left|\frac{x\varepsilon\delta_1}{q}-\tau\right|$，

其中$\tau=q\beta-[q\beta]$。欲使

$$-\frac{1}{3}\leqslant\frac{x}{q}\left(\frac{x\varepsilon\delta_1}{q}-\tau\right)<\frac{1}{3}$$

则须 $\frac{\tau^2}{4\varepsilon\delta_1}-\frac{1}{3}\leqslant\frac{x^2\varepsilon\delta_1}{q^2}-\frac{x\tau}{q}+\frac{\tau^2}{4\varepsilon\delta_1}<\frac{\tau^2}{4\varepsilon\delta_1}+\frac{1}{3}$

$$\frac{\tau^2}{4\varepsilon\delta_1}-\frac{1}{3}\leqslant\left(\frac{x\sqrt{\varepsilon\delta_1}}{q}-\frac{\tau}{2\sqrt{\varepsilon\delta_1}}\right)^2<\frac{\tau^2}{4\varepsilon\delta_1}+\frac{1}{3}$$

只要 $\frac{\tau^2}{4\varepsilon\delta_1}-\frac{1}{3}\geqslant 0$ 即 $\tau^2\geqslant\frac{4\varepsilon\delta_1}{3}$

就有 $\frac{1}{\sqrt{\varepsilon\delta_1}}\left(\frac{\tau}{2\sqrt{\varepsilon\delta_1}}+\sqrt{\frac{\tau^2}{4\varepsilon\delta_1}-\frac{1}{3}}\right)\leqslant\frac{x}{q}<\frac{1}{\sqrt{\varepsilon\delta_1}}\left(\frac{\tau}{2\sqrt{\varepsilon\delta_1}}+\sqrt{\frac{\tau^2}{4\varepsilon\delta_1}+\frac{1}{3}}\right)$。

令

$$\xi_1 = \frac{1}{\sqrt{\varepsilon\delta_1}}\left(\frac{\tau}{2\sqrt{\varepsilon\delta_1}} + \sqrt{\frac{\tau^2}{4\varepsilon\delta_1} - \frac{1}{3}}\right)$$

$$\xi_2 = \frac{1}{\sqrt{\varepsilon\delta_1}}\left(\frac{\tau}{2\sqrt{\varepsilon\delta_1}} + \sqrt{\frac{\tau^2}{4\varepsilon\delta_1} + \frac{1}{3}}\right)$$

下面研究如何才能使$\xi_2 - \xi_1 \geqslant 1$．对不等式

$$\xi_2 - \xi_1 = \frac{1}{\sqrt{\varepsilon\delta_1}}\left(\sqrt{\frac{\tau^2}{4\varepsilon\delta_1} + \frac{1}{3}} - \sqrt{\frac{\tau^2}{4\varepsilon\delta_1} + \frac{1}{3}}\right) > 1$$

求解得 $\tau^2 < \frac{4}{9} + \varepsilon^2\delta_1{}^2$

因此当 $\frac{4\varepsilon\delta_1}{3} \leqslant \tau^2 < \frac{4}{9} + \varepsilon^2\delta_1{}^2$

时，结论已经被证明。

2）当$\tau^2 < \frac{4\varepsilon\delta_1}{3}$时，因$\tau > 0$， $0 < \delta_1 < \frac{1}{\sqrt{5}}$，

$$\xi = \frac{1}{\sqrt{\varepsilon\delta_1}}\left(\frac{\tau}{2\sqrt{\varepsilon\delta_1}} + \sqrt{\frac{\tau^2}{4\varepsilon\delta_1} + \frac{1}{3}}\right)$$

$$> \frac{1}{\sqrt{\varepsilon\delta_1}}\sqrt{\frac{1}{3}} = \sqrt{\frac{1}{3\varepsilon\delta_1}} > \sqrt{\frac{1}{3\varepsilon\cdot\frac{1}{\sqrt{5}}}} > 1$$

（只需取$0 < \varepsilon < \frac{\sqrt{5}}{3}$即可）．

对任一$\eta > 0$，取$\xi_1 = \eta$，$\xi_2 = \xi + \eta$，显然$\xi_2 - \xi_1 = \xi > 1$，故满足$px - qy = [q\beta]$、$\xi_1 q \leqslant x < \xi_2 q$的$x$存在。又

$$\tau^2 < \frac{4\varepsilon\delta_1}{3}\text{即} - \frac{\tau^2}{4\varepsilon\delta_1} > -\frac{1}{3},$$

从而 $\frac{x}{q}\left(\frac{x\varepsilon\delta_1}{q} - \tau\right) =$

$$=\left(\frac{x\sqrt{\varepsilon\delta_1}}{q}-\frac{\tau}{2\sqrt{\varepsilon\delta_1}}\right)^2-\frac{\tau^2}{4\varepsilon\delta_1}>-\frac{1}{3} \tag{1}$$

另一方面，因为$y=ax+b$，故当x在一区间内变化时，y^2在两端点之一取得最大值，因此

$$\frac{x}{q}\left(\frac{x\varepsilon\delta_1}{q}-\tau\right)=\left(\frac{x\sqrt{\varepsilon\delta_1}}{q}-\frac{\tau}{2\sqrt{\varepsilon\delta_1}}\right)^2-\frac{\tau^2}{4\varepsilon\delta_1}$$

$$\leqslant\max\left\{\eta^2\varepsilon\delta_1-\eta\tau,\left(\sqrt{\frac{\tau^2}{4\varepsilon\delta_1}+\frac{1}{3}}+\eta\sqrt{\varepsilon\delta_1}\right)^2-\frac{\tau^2}{4\varepsilon\delta_1}\right\}$$

而如果 $\max\left\{\eta^2\varepsilon\delta_1-\eta\tau,\left(\sqrt{\frac{\tau^2}{4\varepsilon\delta_1}+\frac{1}{3}}+\eta\sqrt{\varepsilon\delta_1}\right)^2-\frac{\tau^2}{4\varepsilon\delta_1}\right\}$

$$=\eta^2\varepsilon\delta_1-\eta\tau$$

则有 $\left(\sqrt{\frac{\tau^2}{4\varepsilon\delta_1}+\frac{1}{3}}+\eta\sqrt{\varepsilon\delta_1}\right)^2-\frac{\tau^2}{4\varepsilon\delta_1}<\eta^2\varepsilon\delta_1-\eta\tau,$

从而 $\frac{1}{3}+2\eta\sqrt{\frac{\tau^2}{4}+\frac{\varepsilon\delta_1}{3}}<-\eta\tau$

此不可能．所以

$$\max\left\{\eta^2\varepsilon\delta_1-\eta\tau,\left(\sqrt{\frac{\tau^2}{4\varepsilon\delta_1}+\frac{1}{3}}+\eta\sqrt{\varepsilon\delta_1}\right)^2-\frac{\tau^2}{4\varepsilon\delta_1}\right\}$$

$$=\left(\sqrt{\frac{\tau^2}{4\varepsilon\delta_1}+\frac{1}{3}}++\eta\sqrt{\varepsilon\delta_1}\right)^2-\frac{\tau^2}{4\varepsilon\delta_1}$$

从而

$$\frac{x}{q}\left(\frac{x\varepsilon\delta_1}{q}-\tau\right)\leqslant\left(\sqrt{\frac{\tau^2}{4\varepsilon\delta_1}+\frac{1}{3}}+\eta\sqrt{\varepsilon\delta_1}\right)^2-\frac{\tau^2}{4\varepsilon\delta_1}$$

也就是

$$\frac{x}{q}\left(\frac{x\varepsilon\delta_1}{q}-\tau\right)\leqslant\frac{1}{3}+\eta^2\varepsilon\delta_1+2\eta\sqrt{\frac{\tau^2}{4}+\frac{\varepsilon\delta_1}{3}} \tag{2}$$

从（1）、（2）我们可以假定

$$\left|\frac{x}{q}\left(\frac{x\varepsilon\delta_1}{q}-\tau\right)-\frac{1}{3}\right|\leqslant\eta^2\varepsilon\delta_1+2\eta\sqrt{\frac{\tau^2}{4}+\frac{\varepsilon\delta_1}{3}}$$

不然的话，就有

$$\frac{x}{q}\left(\frac{x\varepsilon\delta_1}{q}-\tau\right)-\frac{1}{3}>\eta^2\varepsilon\delta_1+2\eta\sqrt{\frac{\tau^2}{4}+\frac{\varepsilon\delta_1}{3}} \quad (3)$$

或 $$\frac{x}{q}\left(\frac{x\varepsilon\delta_1}{q}-\tau\right)-\frac{1}{3}<-\left(\eta^2\varepsilon\delta_1+2\eta\sqrt{\frac{\tau^2}{4}+\frac{\varepsilon\delta_1}{3}}\right) \quad (4)$$

（3）与（2）矛盾；（4）与（1）给出

$$\left|\frac{x}{q}\left(\frac{x\varepsilon\delta_1}{q}-\tau\right)\right|<\frac{1}{3}$$

此种情形结论显然成立．所以

$$\left|\frac{x}{q}\left(\frac{x\varepsilon\delta_1}{q}-\tau\right)-\frac{1}{3}\right|\leqslant\eta^2\varepsilon\delta_1+2\eta\sqrt{\frac{\tau^2}{4}+\frac{\varepsilon\delta_1}{3}}$$

$$<\eta+2\eta=3\eta$$

（只需$0<\eta<1$，$0<\varepsilon<1$）

此即 $$\frac{x}{q}\left(\frac{x\varepsilon\delta_1}{q}-\tau\right)=\frac{1}{3}+O(\eta)$$

由于η可以$\to 0^+$，所以在此种情形下结论是成立的．

3）当$\sqrt{\frac{4}{9}+\varepsilon^2\delta_1^2}\leqslant\tau<1$时，因为

$$\sqrt{\frac{4}{9}+\varepsilon^2\delta_1^2}=\left(\frac{4}{9}\right)^{\frac{1}{2}}+\frac{1}{2}\left(\frac{4}{9}\right)^{\frac{1}{2}-1}\varepsilon^2\delta_1^2+$$

$$+\frac{\frac{1}{2}\left(\frac{1}{2}-1\right)}{2!}\left(\frac{4}{9}\right)^{\frac{1}{2}-2}(\varepsilon^2\delta_1^2)^2+\cdots$$

$$=\frac{2}{3}+\frac{3}{4}\varepsilon^2\delta_1^2-\frac{27}{64}\varepsilon^4\delta_1^4+\cdots$$

所以 $\sqrt{\frac{4}{9}+\varepsilon^2\delta_1^{\ 2}}>\frac{2}{3}+\frac{3}{4}\varepsilon^2\delta_1^{\ 2}-\frac{27}{64}\varepsilon^4\delta_1^{\ 4}$

从而 $$\tau>\frac{2}{3}+\frac{3}{4}\varepsilon^2\delta_1^{\ 2}-\frac{27}{64}\varepsilon^4\delta_1^{\ 4}$$

$$1-\tau<\frac{1}{3}-\frac{3}{4}\varepsilon^2\delta_1^{\ 2}+\frac{27}{64}\varepsilon^4\delta_1^{\ 4}$$

任一$\eta>0$且合条件$(2+\eta)\eta<\delta$之η，可以决定整数对x、y，使其满足条件

$$px-qy=[q\beta]+1,\quad \eta q\leqslant x<(1+\eta)q$$

此时 $|x\theta-y-\beta|=\left|\frac{x\delta_1\varepsilon}{q^2}+\frac{1-\tau}{q}\right|=\frac{1}{q}\left(\frac{x\delta_1\varepsilon}{q}+(1-\tau)\right)$

$$<\frac{1}{q}\left\{(1+\eta)\delta_1\varepsilon+\frac{1}{3}-\frac{3}{4}\varepsilon^2\delta_1^{\ 2}+\frac{27}{64}\varepsilon^4\delta_1^{\ 4}\right\}$$

其中$\tau=q\beta-[q\beta]$。由于ε可以任意小，总可以选取η，使之满足

$$\eta>3\left\{(1+\eta)\delta_1\varepsilon+\frac{27}{64}\varepsilon^4\delta_1^{\ 4}\right\}$$

因此 $$\frac{\eta}{3}>\left\{(1+\eta)\delta_1\varepsilon-\frac{3}{4}\varepsilon^2\delta_1^{\ 2}+\frac{27}{64}\varepsilon^4\delta_1^{\ 4}\right\}$$

从而 $$\frac{1+\eta}{3}>\left\{(+\eta)\delta_1\varepsilon+\frac{1}{3}-\frac{3}{4}\varepsilon^2\delta_1^{\ 2}+\frac{27}{64}\varepsilon^4\delta_1^{\ 4}\right\}$$

所以 $|x\theta-y-\beta|<\frac{1}{q}\left\{(1+\eta)\delta_1\varepsilon+\frac{1}{3}-\frac{3}{4}\varepsilon^2\delta_1^{\ 2}+\frac{27}{64}\varepsilon^4\delta_1^{\ 4}\right\}$

$$<\frac{1}{q}\cdot\frac{1+\eta}{3}<\frac{(1+\eta)^2}{3x}=\frac{1+(2+\eta)\eta}{3x}$$

又因为$(2+\eta)\eta<\delta$，故

$$|x\theta-y-\beta|<\frac{1+\delta}{3x}.$$

第十一章　不定方程

一、提　　要

定理 1　不定方程

$$a_1x_1+a_2x_2+\cdots+a_nx_n=N$$

可解的充分必要条件是

$$(a_1,a_2,\cdots,a_n)\mid N。$$

定理 2　设 $(a_1,a_2,\cdots,a_n)=1$，命$A(N)$表方程

$a_1x_1+a_2x_2+\cdots+a_nx_n=N$，$a>0$，$x\geqslant 0$ 的解数，则

$$\lim_{N\to\infty}\frac{A(N)}{N^{n-1}}=\frac{1}{a_1a_2\cdots a_n\,(n-1)!}.$$

定义　称二次不定方程

$$ax^2+bxy+cy^2=k$$

合条件$(x,y)=1$的解(x,y)为既约解，其中$d=b^2-4ac$非平方数且 $(a,b,c)=1$。

定理 3　若x、y为一既约解，则可唯一定出二整数s及r，使

$$xs-yr=1$$

及　　$$l=(2ax+by)r+(bx+2cy)s$$

适合　$l^2\equiv d\pmod{4k}$，$0\leqslant l<2k$。

定理 4　若(x_1,y_1)、(x_2,y_2)为对应于同一l的二既约解，则有

$$2ax_1+(b+\sqrt{d})y_1=(2ax_2+(b+\sqrt{d})y_2)\left(\frac{t+u\sqrt{d}}{2}\right).$$

此处，t及u为

$$t^2-du^2=4$$

的整数解。反过来，若(x_2, y_2)是一既约解，则由上式所定义的(x_1, y_1)也为一既约解，且有相同的l。

定理 5　设$d<0$，命

$$w=\begin{cases}2，若 d<-4\\4，若 d=-4\\6，若 d=-3\end{cases}$$

则不定方程　$ax^2+bxy+cy^2=k$

有w个既约解对应于同一l。

定义　设$d>0$，称不定方程

$$ax^2+bxy+cy^2=k$$

适合条件

$$2ax+(b-\sqrt{d})y>0,\quad 1\leqslant\left|\frac{2ax+(b+\sqrt{d})y}{2ax+(b-\sqrt{d})y}\right|<\varepsilon^2$$

的解为原解。其中ε是$x^2-dy^2=4$的基本解。

定理 6　设$d>0$，对应于同一l，不定方程

$$ax^2+bxy+by^2=k$$

如果有既约原解，则只有唯一既约原解。

定理 7　对应于同一l，不定方程

$$ax^2+bxy+cy^2=k$$

如果有既约原解，则只有w个。

定理 8　不定方程

$$x^2+y^2=z^2$$

满足$(x,y)=1$、$x>0$、$y>0$、$z>0$、$(x, y)=1$、$2|x$的全部整数解可表为

$$x=2ab,\ y=a^2-b^2,\ z=a^2+b^2,$$
$$(a,\ b)=1,\ a>b>0,\ a+b\equiv 1 \pmod 2.$$

定理9 在非直线的有有理系数的二次曲线上如有一有理点，则有无穷个有理点。

定理10 设A、B、C是不全为零的有理数。若B^2-4AC为一平方数，则二次曲线

$$A\xi^2+B\xi\eta+C\eta^2+D\xi+E\eta+F=0$$

上有无穷个有理点。

定理11 不定方程

$$x^4+y^4=z^2,\ x>0,\ y>0$$

无整数解。

无穷递降法使用步骤如下：

（1）若一命题$P(n)$对若干正整数n正确，则在这些n中必有最小的。

（2）若$P(n)$正确，则有一正整数$n'<n$，使$P(n')$也正确。若此二步已证，则命题$P(n)$决不成立。

定义 不定方程

$$x^2+y^2+z^2=3xyz$$

的解名为Марков数。

定理12 若x_0、y_0、z_0是不定方程

$$x^2+y^2+z^2=3xyz$$

的解，则x_0、y_0、$3x_0y_0-z_0$也是。

定理13 不定方程

$$W^3+3W(X^2+Y^2+Z^2)+6XYZ=0$$

的有理数解为

$W=-6\rho abc,\ X=\rho a(a^2+3b^2+3c^2)$,

$Y=\rho b(a^2+3b^2+9c^2)$, $Z=3\rho c(a^2+b^2+3c^2)$，此处$(a,b,c)=1$，且ρ为有理数。

定理14　任给一正整数r，必有一数N存在，可以用r种方法表为二立方数的和。

定理15　若$C \neq 0$，则三次曲面

$$\zeta^2 = \xi^3 + A\xi + B + C\eta^2$$

上有无穷多个有理点，此处A、B、C为有理数。

定理16　设$f(\xi, \eta)$是一有理系数的三次多项式，但不能用一次变形变为只有一个变数的多项式，则三次曲面

$$\zeta^2 = f(\xi, \eta)$$

上有无穷多个有理点。

定理17　命$S_2(\xi, \eta, \zeta)$及$T_2(\xi, \eta, \zeta)$为ξ、η、ζ的二次齐次式，则三次曲面

$$\zeta S_2(\xi, \eta, \zeta) + T_2(\xi, \eta, \zeta) + \zeta = 0$$

上有无穷多个有理点。

定理18　若非锥面及柱面的三次曲面上有一有理点，则有无穷多个有理点。

二、题　　解

§ 2　一次不定方程

习题　若$(a, b) = 1$，$a > 0$，$b > 0$，则

$$ax + by = N,\quad x \geqslant 0,\quad y \geqslant 0$$

之解数为

$$\frac{N - (bl + am)}{ab} + 1$$

此处之l为$bl \equiv N \pmod{a}$之最小非负解答，又m为$am \equiv N \pmod{b}$之最小非负解答。

证：设x_0、y_0是合条件$x\geqslant 0$、$y\geqslant 0$且x_0最小的一组解，则

$$x=x_0+bt,\quad y=y_0-at$$

给出$ax+by=N$的全部整数解，此处t是整数．设y_0是最大的一个，从而$y=y_0-at$给出

$$0\leqslant t=\frac{y_0}{a}-\frac{y}{a}\leqslant\left[\frac{y_0}{a}\right]$$

又由　$bl\equiv N(\bmod a)$，$am\equiv N(\bmod b)$

有　$$N=ar+bl,\quad N=bT+am$$

从l、m均为非负最小解答知道

$$y_0=T=\frac{N-am}{b}$$

显然也有$l<a$．若不然，由

$$ar+bl=N$$

知道r、l是　$$ax+by=N$$

的一组非负解且l是最小者，而

$$ax+by=N$$

的全部解可由

$$x=r+sb,\quad y=l-sa$$

给出．取$s=1$，$y=l-a\geqslant 0$仍是它的解，此与l最小矛盾．另一方面，由题设条件有

$$N\equiv bl\equiv bl+am\ (\bmod a)$$

$$N\equiv am\equiv am+bl(\bmod b)$$

结合条件$(a,\ b)=1$可得

$$N\equiv am+bl(\bmod ab)$$

此即　$$ab\mid N-(am+bl)$$

故$\dfrac{N-(am+bl)}{ab}$是整数．又因为

$$\frac{y_0}{a}=\frac{T}{a}=\frac{N-am}{ab}=\frac{N-(am+bl)}{ab}+\frac{l}{a}$$

且$l<a$，$\left[\frac{l}{a}\right]=0$，从而就有

$$\left[\frac{y_0}{a}\right]=\left[\frac{N-(am+bl)}{ab}+\frac{l}{a}\right]=\frac{N-(am+bl)}{ab}+\left[\frac{l}{a}\right]$$

$$=\frac{N-(am+bl)}{ab},$$

所以 $0\leqslant t\leqslant\left[\frac{y_0}{a}\right]=\frac{N-(am+bl)}{ab}$

故t可取$\frac{N-(am+bl)}{ab}+1$个值，此即合题设条件的解数为

$$\frac{N-(am+bl)}{ab}+1.$$

§ 4 解$ax^2+bxy+cy^2=k$

习题 1 如上述之假定，证明

$$0<y\leqslant\left(\varepsilon-\frac{1}{\varepsilon}\right)\sqrt{ak/d}.$$

证："如上述之假定"系指方程

$$ax^2+bxy+cy^2=k>0$$

合条件： $a>0$，$b>0$，$d=b^2-4ac>0$，

$L=2ax+(b+\sqrt{d})y$，$\overline{L}=2ax+(b-\sqrt{d})y$，

$$L>\overline{L}>0,\quad 1\leqslant\left|\frac{L}{\overline{L}}\right|<\varepsilon^2,\quad \varepsilon=\frac{x_0+y_0\sqrt{d}}{2},$$

$x_0+y_0\sqrt{d}$为$X^2-dY^2=4$的基本解。

今有 $\qquad \bar{L}=\dfrac{4ak}{L}$

因此 $\qquad 0<2\sqrt{d}\,y=L-\bar{L}=L-\dfrac{4ak}{L}$

$$=\sqrt{L\bar{L}\frac{L}{\bar{L}}}-\frac{4ak}{\sqrt{L\bar{L}\frac{L}{\bar{L}}}}$$

结合条件 $1\leqslant\left|\dfrac{L}{\bar{L}}\right|=\dfrac{L}{\bar{L}}<\varepsilon^2$

有 $\qquad \sqrt{L\bar{L}\dfrac{L}{\bar{L}}}\leqslant\varepsilon\sqrt{4ak}$，

从而 $\quad 0<2\sqrt{d}\,y\leqslant\varepsilon\sqrt{4ak}-\dfrac{4ak}{\varepsilon\sqrt{4ak}}=\left(\varepsilon-\dfrac{1}{\varepsilon}\right)\sqrt{4ak}$，

故 $\qquad 0<y\leqslant\left(\varepsilon-\dfrac{1}{\varepsilon}\right)\sqrt{ak/d}$

习题 2 证明

$$x_1=\frac{t-bu}{2}x-cuy,\quad y_1=aux+\frac{t+bu}{2}y$$

变$ax^2+bxy+cy^2$为$ax_1{}^2+bx_1y_1+cy_1{}^2$。

证： $ax_1{}^2+bx_1y_1+cy_1{}^2$

$$=a\left(\frac{t-bu}{2}x-cuy\right)^2$$

$$+b\left(\frac{t-bu}{2}x-cuy\right)\left(aux+\frac{t+bu}{2}y\right)$$

$$+c\left(aux+\frac{t+bu}{2}y\right)^2$$

$$=\left[\frac{a(t-bu)^2}{4}+\frac{(t-bu)}{2}abu+a^2cu^2\right]x^2$$

$$+\left[acu(t+bu)+\frac{b(t^2-b^2u^2)}{4}-abcu^2-acu(t-bu)\right]xy$$

$$+\left[ac^2u^2-\frac{bcu(t+bu)}{2}+\frac{c(t+bu)^2}{4}\right]y^2 \qquad (1)$$

由$d=b^2-4ac$且$t^2-du^2=4$，因此

$$\frac{a(t-u)^2}{4}+\frac{(t-bu)}{2}abu+a^2cu^2$$

$$=a\left(\frac{t^2-2btu+b^2u^2}{4}+\frac{2btu-2b^2u^2}{4}+\frac{4a^2cu^2}{4}\right)$$

$$=\frac{a}{4}(t^2+4acu^2-b^2u^2)$$

$$=\frac{a}{4}(t^2-du^2)=a; \qquad (2)$$

$$acu(t+bu)+\frac{b(t^2-b^2u^2)}{4}-abcu^2-acu(t-bu)$$

$$=abcu^2+\frac{bt^2-b^3u^2}{4}$$

$$=\frac{b}{4}(4acu^2+t^2-b^2u^2)$$

$$=\frac{b}{4}(t^2-du^2)=b; \qquad (3)$$

$$ac^2u^2-\frac{bcu(t+bu)}{2}+\frac{c(t+bu)^2}{4}$$

$$=ac^2u^2-\frac{bctu+b^2cu^2}{2}+\frac{ct^2+2bctu+b^2cu^2}{4}$$

$$=\frac{c}{4}(t^2+4acu^2-bu^2)$$

$$=\frac{c}{4}(t^2-du^2)=c. \qquad (4)$$

把（2）、（3）、（4）代入（1）可得

$$ax_1^2+bx_1y_1+cy_1^2=ax^2+bxy+cy^2$$

也就是变换 $x_1=\frac{t-bu}{2}x-cuy$，$y_1=aux+\frac{t+bu}{2}y$

把$ax^2+bxy+cy^2$变为$ax_1^2+bx_1y_1+cy_1^2$。

§5 求解方法

习题1 求下列诸不定方程之诸解：

(a) $3x^2-8xy+7y^2-4x+2y=109$

(b) $3xy+2y^2-4x-3y=12$

(c) $9x^2-12xy+4y^2+3x+2y=12$

(d) $x^2-8xy-17y^2+72y-75=0$。

解：(a) 设

$$X=3x-4y-2,\ Y=5y-5$$

方程(a) 就变形为

$$5X^2+Y^2=1680 \qquad (a')$$

(a′) 有以下8组解：

(4，40)，(4，−40)，(−4，40)，(−4，−40)，

(16，20)，(16，−20)，(−16，20)，(−16，−20)。

从而方程(a)的所有解由下面8个方程组给出：

（1）$\begin{cases}X=4\\Y=40\end{cases}$ （2）$\begin{cases}X=4\\Y=-40\end{cases}$ （3）$\begin{cases}X=-4\\Y=40\end{cases}$ （4）$\begin{cases}X=-4\\Y=-40\end{cases}$

（5）$\begin{cases}X=16\\Y=20\end{cases}$ （6）$\begin{cases}X=16\\Y=-20\end{cases}$ （7）$\begin{cases}X=-16\\Y=20\end{cases}$ （8）$\begin{cases}X=-16\\Y=-20\end{cases}$

方程组（2）、（3）、（5）、（8）均无解。方程组（1）给出解(14，9)，（4）给出解(−10，−7)，（6）给出解(2，−3)，（7）给出解(2，5)。所以方程(a)只有四组解：

(14, 9)，(−10，−7)，(2，−3)，(2，5)．

(b) 可变形为 $x=\dfrac{-2y^2+3y+12}{3y-4}$

$$9x=-6y+1+\frac{112}{3y-4} \qquad (b')$$

(b′)给出$3y-4|112$，又因$112=2^4\cdot 7$，故$\dfrac{112}{3y-4}$可能取±1、

±2、±4、±7、±8、±14、±16、±28、±56、±112.

但(b′)又给出$3|1+\dfrac{112}{3y-4}$，故$\dfrac{112}{3y-4}$只可能为

−1、2、−4、−7、8、14、−16、−28、56、−112.

因此$3y-4$只能等于

−112、56、−28、−16、14、8、−7、−4、2、−1.

故y等于

−36、20、−8、−4、6、4、−1、0、2、1.

代入(b)知x等于

24、−13、5、2、−3、−1、−1、−3、5、−13.

所以方程(b)有下列10组解：(24，−36)，(−13，20)，(5，−8)，(2，−4)，(−3，6)，(−1，4)，(−1，−1)，(−3，0)，(5，2)，(−13，1)．

(c)解关于x的方程得

$$x=\frac{(12y-3)\pm\sqrt{(12y-3)^2-36(4y^2+2y-12)}}{18}$$

$$=\frac{(4y-1)\pm\sqrt{49-16y}}{6}$$

设$49-16y=t^2$，则有

$$x=\frac{4y-1\pm t}{6} \qquad (1)$$

$$y=3-\frac{t^2-1}{16} \qquad (2)$$

（2）给出$16|t^2-1$，从而设$t=2k_1-1$，有

$$\frac{t^2-1}{16}=\frac{(2k_1-1)^2-1}{16}=\frac{k_1(k_1-1)}{4}$$

如果设$k_1-1=4k_2$即$k_1=4k_2+1$，则

$$t=8k_2+1;$$

如果设$k_1=4k_2$，则

$$t=8k_2-1.$$

（一） 当$t=8k_2+1$时，由（1）、（2）得

$$x=2-2k_2{}^2-\frac{2k_2(k_2-1)}{3} \qquad (3)$$

或

$$x=1-2k_2{}^2-2k_2-\frac{2(k_2+1)(k_2-1)}{3} \qquad (4)$$

$$y=3-4k_2{}^2-k_2 \qquad (5)$$

(i)设$k_2=3k_3$，分别代入（3）、（5）得

$$\begin{cases}x=-24k_3{}^2+2k_3+2\\ y=-36k_3{}^2-3k_3+3\end{cases} \qquad (6)$$

代入（4）无整数解。

(ii)设$k_2=3k_3+1$，代入（3）、（4）、（5）得两组解

$$\begin{cases}x=-24k_3{}^2-14k_3\\ y=-36k_3{}^2-27k_3-2\end{cases} \qquad (7)$$

$$\begin{cases}x=-24k_3{}^2-22k_3-3\\ y=-36k_3{}^2-27k_3-2\end{cases} \qquad (8)$$

(iii) 设$k_3=3k_2+2$，代入（3）无解，代入（4）得

$$\begin{cases}x=-24k_3^2-38k_3-13\\y=-36k_3^2-51k_3-15\end{cases} \quad (9)$$

（二）当$t=8k_2-1$时，由（1）、（2）得

$$x=1-2k_2^2+2k_2-\frac{2(k_2+1)(k_2-1)}{3} \quad (10)$$

或 $$x=2-2k_2^2-\frac{2k_2(k_2+1)}{3} \quad (11)$$

$$y=3-4k_2^2+k_2 \quad (12)$$

(i) 设$k_2=3k_3$，代入(10)无解．代入(11)、(12)得

$$\begin{cases}x=-24k_3^2-2k_3+2\\y=-36k_3^2+3k_3+3\end{cases} \quad (13)$$

(ii) 设$k_2=3k_3+1$，代入(10)、(12)得

$$\begin{cases}x=-24k_3^2-10k_3+1\\y=-36k_3^2-21k_3\end{cases} \quad (14)$$

代入(11)无解．

(iii) 设$k_2=3k_3+2$，代入(10)、(11)、(12)得二组解

$$\begin{cases}x=-24k_3^2-26k_3-5\\y=-36k_3^2-45k_3-11\end{cases} \quad (15)$$

$$\begin{cases}x=-24k_3^2-34k_3-10\\y=-36k_3^2-45k_3-11\end{cases} \quad (16)$$

综上所述，方程(c)的解由（6）、（7）、（8）、（9）、(13)、(14)(15)、(16)诸式给出．

(d) 设$X=33y-36$，$Y=x-4y$

则方程(d)变形为 $X^2-33Y^2=-1179$

方程$x^2-33y^2=1$的基本解为

$$x_0 - y_0\sqrt{33} = 23 + 4\sqrt{33}$$

而方程$X^2 - 33Y^2 = -1179$任一类的基本解

$$u_0 + v_0\sqrt{33}$$

必须满足 $0 < v_0 \leqslant \dfrac{y_0}{\sqrt{2(x_0 - 1)}}\sqrt{N}$

又因为$x_0 = 23$、$y_0 = 4$、$N = 1179$，故可得

$$0 < v_0 \leqslant \frac{4}{\sqrt{2(23-1)}}\sqrt{1179} < 21$$

但在$0 < v_0 \leqslant 20$的范围内只有

$$u_0 + v_0\sqrt{33} = 3 + 6\sqrt{33}$$

为方程 $X^2 - 33Y^2 = -1179$

的解，从而$X^2 - 33Y^2 = -1179$只有一类解．故全体解由

$$X + Y\sqrt{33} = \pm(3 + 6\sqrt{33})(23 + 4\sqrt{33})^n$$

给出，其中n为整数．又因为

$$X = 33y - 36,\quad y = x - 4y$$

故方程(d)的全体解由下式给出

$$(33y - 36) + (x - 4y)\sqrt{33} = \pm(3 + 6\sqrt{33})(23 + 4\sqrt{33})^n$$

其中n仍然为整数．

习题 2 设$k < \sqrt{d}$．求证

$$ax^2 + bxy + cy^2 = k$$

之解，可由$ax^2 + bx + c = 0$

之根之渐近分数得之．试推广本节之结果．

证： 显然必须假定d为非平方数且$k \neq 0$，因此$ac \neq 0$；还可进一步假定$k > 0$，否则可用-1乘$ax^2 + bxy + cy^2 = k$，再设$a' = -a$、$b' = -b$、$c' = -c$、$k' = -k$，则$ax^2 + bxy + cy^2 = k$就变形为$a'x^2 + b'xy + c'y^2 = k'$，而$k' > 0$。

设$(x, y) = (p, q)$ 是$ax^2 + bxy + cy^2 = k$的一组整数解，且合

条件$p>0$、$q>0$、$(p,q)=1$。

(一) 先证 $\frac{p}{q}>\alpha_1$ 或 $\frac{p}{q}<\alpha_2$。 (1)

其中 $\alpha_1=\frac{-b+\sqrt{d}}{2a}$，$\alpha_2=\frac{-b-\sqrt{d}}{2a}$

它们是$f(x)=ax^2+bx+c$的根．由

$$ap^2+bpq+cq^2=k$$

得 $$p=\frac{-bq\pm\sqrt{b^2q^2-4acq^2+4ak}}{2a}$$

即 $$\frac{p}{q}=\frac{-b\pm\sqrt{d+4ak/q^2}}{2a}$$

当$a>0$时

$$\frac{p}{q}=\frac{-b+\sqrt{d+4ak/q^2}}{2a}>\frac{-b+\sqrt{d}}{2a}=\alpha_1$$

$$\frac{p}{q}=\frac{-b-\sqrt{d+4ak/q^2}}{2a}<\frac{-b-\sqrt{d}}{2a}=\alpha_2$$

当$a<0$时

$$\frac{p}{q}\cdot 2a=-b+\sqrt{d+4ak/q^2}<-b+\sqrt{d},$$

$$\frac{p}{q}>\frac{-b+\sqrt{d}}{2a}=\alpha_1$$

$$\frac{p}{q}\cdot 2a=-b-\sqrt{d+4ak/q^2}>-b-\sqrt{d},$$

$$\frac{p}{q}<\frac{-b-\sqrt{d}}{2a}=\alpha_2$$

故(1)成立。

(二) 再证$a>0$时，或者$a<0$、$c<0$时

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^2}. \qquad (2)$$

其中α是$f(x)=ax^2+bx+c$的根。当$a>0$时，有$\alpha_2<\alpha_1$。

如果$\frac{p}{q}<\alpha_2$，对$f(x)$在$\left[\frac{p}{q},\ \alpha_2\right]$上使用Lagrange中值定理：

$$f(\alpha_2)-f\left(\frac{p}{q}\right)=f'(\xi)\left(\alpha_2-\frac{p}{q}\right),\ \frac{p}{q}\leqslant\xi\leqslant\alpha_2.$$

因为$f(\alpha_2)=0$，$f\left(\frac{p}{q}\right)=\frac{k}{q^2}$，$f'(\xi)=2a\xi+b$，得

$$\alpha_2-\frac{p}{q}=\frac{-k}{(2a\xi+b)}\cdot\frac{1}{q^2}$$

由于$\left|\alpha_2-\frac{p}{q}\right|=\alpha_2-\frac{p}{q}$，从而要想$\left|\alpha_2-\frac{p}{q}\right|<\frac{1}{q^2}$，只需$\frac{-k}{2a\xi+b}<1$即$\xi<\frac{-b-k}{2a}$就可以了。而$\xi<\frac{-b-k}{2a}$是显然的，可以从$k<\sqrt{d}$、$\alpha_2=\frac{-b-\sqrt{d}}{2a}<\frac{-b-k}{2a}$和$\xi\leqslant\alpha_2$立得。这就证明，$\frac{p}{q}<\alpha_2$时，

$$\left|\alpha_2-\frac{p}{q}\right|<\frac{1}{q^2} \qquad (3)$$

如果$\frac{p}{q}>\alpha_1$，则对$f(x)$在$\left[\alpha_1,\ \frac{p}{q}\right]$上用Lagrange中值定理一样地可以证明

$$\left|\alpha_1-\frac{p}{q}\right|<\frac{1}{q^2} \qquad (4)$$

当$a<0$、$c<0$时，有

$$\frac{-b+\sqrt{d}}{2a}=\alpha_1<\alpha_2=\frac{-b-\sqrt{d}}{2a}$$

由(一)的(1)得

$$\frac{-b+\sqrt{d}}{2a}\leqslant\frac{p}{q}\leqslant\frac{-b-\sqrt{d}}{2a} \tag{5}$$

下面再进一步证明

$$\frac{-b+k}{2a}<\frac{p}{q}<\frac{-b-k}{2a} \tag{6}$$

不能成立。否则，用与（一）完全相同的方法可得

$$\frac{-b+k}{2c}<\frac{q}{p}<\frac{-b-k}{2c} \tag{6'}$$

容易验证$\frac{-b+k}{2a}>0$，否则$\frac{-b-k}{2a}<0$，这就与$\frac{-b-k}{2a}>\frac{p}{q}>0$相矛盾了。同理$\frac{-b+k}{2c}>0$，从而(6′)给出

$$\frac{2c}{-b-k}<\frac{p}{q}<\frac{2c}{-b-k} \tag{7}$$

由于a、c的对称性，反过来从（7）也可以推出(6)，此即(6)与(7)等价，故得

$$\frac{-b+k}{2a}=\frac{2c}{-b-k}$$

和

$$\frac{-b-k}{2a}=\frac{2c}{-b+k}$$

但此二式均给出　$b^2-k^2=4ac$

设与题设$k<\sqrt{d}$是相矛盾的，故(6)确实不能成立。因而(5)给出

$$a_1=\frac{-b+\sqrt{d}}{2a}\leqslant\frac{p}{q}\leqslant\frac{-b+k}{2a}$$

或者

$$\frac{-b-k}{2a}\leqslant\frac{p}{q}\leqslant\frac{-b-\sqrt{d}}{2a}=a_2$$

用与前面相同的方法即分别在区间$\left[\alpha_1, \frac{p}{q}\right]$和区间$\left[\frac{p}{q}, \alpha_2\right]$上对$f(x)$使用Lagrange中值定理，可得

$$\left|\alpha_1-\frac{p}{q}\right|<\frac{1}{q^2} \tag{8}$$

或者

$$\left|\alpha_2-\frac{p}{q}\right|<\frac{1}{q^2} \tag{9}$$

从(3)、(4)、(8)、(9)便可以得到(2)。

（三）下面证明$a>0$或$a<0$、$c<0$时，本题结论成立。由(2)可设

$$\alpha-\frac{p}{q}=\frac{\varepsilon\theta}{q^2}, \varepsilon=\pm 1, 0<\theta<1$$

命
$$\frac{p}{q}=[a_0, a_1, \cdots, a_{n-1}]=\frac{p_{n-1}}{q_{n-1}}, \quad (-1)^{n-1}=\varepsilon$$

（因$\frac{p}{q}$展成连分数有两种方法，即n偶或n奇，故可取$(-1)^{n-1}=\varepsilon$）

就有
$$\alpha-\frac{p_{n-1}}{q_{n-1}}=\frac{\varepsilon\theta}{q_{n-1}^2}$$

由次式定义β：

$$\alpha=\frac{p_{n-1}\beta+p_{n-2}}{q_{n-1}\beta+q_{n-2}} \tag{10}$$

如是，则有

$$\frac{\varepsilon\theta}{q_{n-1}^2}=\frac{p_{n-1}\beta+p_{n-2}}{q_{n-1}\beta+q_{n-2}}-\frac{p_{n-1}}{q_{n-1}}=\frac{(-1)^{n-1}}{q_{n-1}(q_{n-1}\beta+q_{n-2})}$$

故
$$\theta=\frac{q_{n-1}}{q_{n-1}\beta+q_{n-2}}$$

解此式可得 $\beta=\frac{q_{n-1}-\theta q_{n-2}}{\theta q_{n-1}}$

因为$0<\theta<1$，故$\beta>0$，而(10)就是

$$\alpha=[a_0,a_1,\cdots,a_{n-1},\beta] \tag{10'}$$

若$\beta\geqslant1$，则

$$\beta=\alpha_n',\quad \alpha_n'=[a_n,a_{n+1},\ \cdots]$$

即$\frac{p}{q}=\frac{p_{n-1}}{q_{n-1}}$为$\alpha$的渐近值。若$\beta<1$，因$\beta>0$可知

$$\left[a_{n-1}+\frac{1}{\beta}\right]=a_{n-1}+c,\quad c\geqslant1$$

即 $\alpha=[a_0,\cdots,a_{n-2},\ a_{n-1}+c,\ \cdots]$

也就是说，$[a_0,\cdots,a_{n-1}]$不是α的渐近值，因此$\beta\geqslant1$是$\frac{p}{q}$为α的渐近值的必要充分条件。现在来证明$\beta>1$。

把(10)代入$ax^2+bx+c=0$得

$$A_n\beta^2+B_n\beta+C_n=0 \tag{11}$$

其中
$$A_n=ap_{n-1}^2+bp_{n-1}q_{n-1}+cq_{n-1}^2$$
$$B_n=2ap_{n-1}p_{n-2}+b(p_{n-1}q_{n-2}+p_{n-2}q_{n-1})+2cq_{n-1}q_{n-2}$$
$$C_n=ap_{n-2}^2+bp_{n-2}q_{n-2}+cq_{n-2}^2$$

直接计算可得

$$B_n^2-4A_nC_n=(b^2-4ac)(p_{n-1}q_{n-2}-p_{n-2}q_{n-1})^2=b^2-4ac$$

再由 $\frac{p}{q}=\frac{p_{n-1}}{q_{n-1}}$

可知$A_n=k$。解(11)得

$$\beta=\frac{-B_n\pm\sqrt{B_n^2-4A_nC_n}}{2A_n}=\frac{-B_n\pm\sqrt{d}}{2k}$$

设 $\beta_1=\frac{-B_n+\sqrt{d}}{2k}$，$\beta_2=\frac{-B_n-\sqrt{d}}{2k}$

从(10′) 得　$\alpha_1=[a_0,a_1,\cdots,a_{n-1},\beta_1]$

$\alpha_2=[a_0,a_1,\cdots,a_{n-1},\beta_2]$

或　$\alpha_1=[a_0,a_1,\cdots,a_{n-1},\beta_2]$

$\alpha_2=[a_0,a_1,\cdots,a_{n-1},\beta_1]$

由$\beta>0$即$\dfrac{-B_n+\sqrt{d}}{2k}>0$，$\dfrac{-B_n-\sqrt{d}}{2k}>0$，且$A_n=k>0$

可知，$C_n>0$，$B_n<0$. 从而

$$4A_nC_n=B_n^2-d>0$$

$$B_n^2>d$$

$$B_n<-\sqrt{d}$$

如果取$\beta=\beta_1=\dfrac{-B_n+\sqrt{d}}{2A_n}$，那么从$-B_n+\sqrt{d}>2\sqrt{d}$、

$2A_n=2k<2\sqrt{d}$立刻得到

$$\beta>1$$

故当$a>0$时，或者$a<0$、$c<0$时，$\dfrac{p}{q}$的确是

$$ax^2+bx+c=0$$

的根的渐近分数.

（四）最后证明$a<0$、$c>0$时习题结论也成立.

由前面所证知道$\dfrac{q}{p}$是方程

$$a+by+cy^2=0$$

的根的渐近分数. 如设δ是$a+by+cy^2=0$的根，就有$\delta=\dfrac{1}{\alpha}$.因此

$\dfrac{q}{p}$若是δ的渐近分数的话，那么$\dfrac{p}{q}$就是α的渐近分数.

综上所述，我们证明了

$$ax^2+bxy+cy^2=k,\ \ k<\sqrt{d}$$

的解，可由

$$ax^2+bx+c=0$$

的根的渐近分数得出.

必须着重指出，当d为平方数时，习题结论就不能成立了.例如$-x^2+4xy=4$对应的$\alpha=0$，4；而$x=2$、$y=1$是$-x^2+4xy=4$的一组解，但$\frac{2}{1}$或$\frac{1}{2}$既不是$\alpha=0$的渐近分数，也不是$\alpha=4$的渐近分数。当d为非平方数时，若$k=0$，容易证明$ax^2+bxy+cy^2=0$只有零解。

我们可以将本节结果作如下一些推广：

(A) 方程

$$ax^2+bxy+cy^2+dx+ey+f=0 \tag{A_1}$$

在$D=b^2-4ac>0$且非平方数，$k<\sqrt{d}$（k在下面确定）的条件下，其解也可通过方程

$$ax^2+bx+c=0$$

的根的渐近分数而得到。以D^2乘(A_1)得

$$aD^2x^2+bD^2xy+cD^2y^2+dD^2x+eD^2y+fD^2=0.$$

命

$$Dx=x'+2cd-be$$

$$Dy=y'+2ae-bd$$

代入上式得

$$\begin{aligned}&a(x'+2cd-be)^2+b(x'+2cd-be)(y'+2ae-bd)\\&+c(y'+2ae-bd)^2+dD(x'+2cd-be)\\&+eD(y'+2ae-bd)+fD^2=0\end{aligned}$$

即

$$ax'^2+bx'y'+cy'^2=k$$

此处

$$\begin{aligned}-k=&a(2cd-be)^2+b(2cd-be)(2ae-bd)\\&+c(2ae-bd)^2+dD(2cd-be)\\&+eD(2ae-bd)+fD^2\end{aligned}$$

再由前面本题的证明可知，此推广是正确的。

(*B*) 方程

$$ax^2+bxy+cy^2=k \tag{B_1}$$

的解可以通过求$\sqrt{d}$的渐近分数而得到。

(B_1) 可以变形为

$$(2ax+by)^2-dy^2=4ak$$

设$u=2ax+by$，$v=y$，则又变形为

$$u^2-dv^2=4ak$$

由关于*Pell*方程熟知的结果可知

$$u^2-dv^2=4ak$$

的所有解可从$\sqrt{d}$的渐近分数逐一求出，即必然存在n，合条件

$$p_{n-1}{}^2-dq_{n-1}{}^2=(-1)^nQ_n\text{，}\quad(-1)^nQ_n=4ak$$

如果设$\sqrt{d}$的循环周期为l，则有

$$p_{ml+n-1}{}^2-dq_{ml+n-1}{}^2=4ak$$

即 $$u=\pm p_{ml+n-1}\text{，}\quad v=\pm q_{ml+n-1}$$

是方程$u^2-dv^2=4ak$的全部解。又因为

$$u=2ax+by\text{，}\quad v=y$$

故不定方程 (B_1) 的全部解存在于

$$x=\frac{-b(\pm q_{ml+n-1})\pm p_{ml+n-1}}{2a}$$

$$y=\pm q_{ml+n-1}$$

之中，因此方程 (B_1) 的解可通过求$\sqrt{d}$的渐近分数而得到。

由(*A*)和(*B*)可以得到：

(*C*)方程

$$ax^2+bxy+cy^2+dx+ey+f=0$$

的解可以通过求$\sqrt{D}$的渐近分数而得到。

(*D*) 关于方程

$$ax^2+bxy+cy^2=k$$

的整数解的个数，还有下面较一般性的定理：

当$d=0$，$a=0$时，无限个解或无解；

当$d=0$，$a\neq 0$时，无限个解或无解；

当$d<0$时，有限个解或无解；

当$d>0$，d是平方数，$k=0$时，无限个解；

当$d>0$，d是平方数，$k\neq 0$时，有限个解或无解；

当$d>0$，d非平方数，$k=0$时，只有零解$x=y=0$；

当$d>0$、d非平方数、$k\neq 0$时，有无限个解或无解.

§ 6 商高定理之推广

习题1 解不定方程

$$x^2+y^2=z^4$$

并证明其解能适合

$x>0$、$y>0$、$z>0$、$(x,y)=1$，$2|x$者，由次式与之：

$x=4ab|a^2-b^2|$*，$y=|a^4+b^4-6a^2b^2|$，

$z=a^2+b^2$，$a>0$，$b>0$，$(a,b)=1$，$a+b\equiv 1 \pmod 2$.

证：设x、y、z为方程$x^2+y^2=z^4$的一组解，并且合条件

$x>0$，$y>0$，$z>0$，$(x,y)=1$，$2|x$

那么 $x=2a_1b_1$，$y=a_1^2-b_1^2$，$z^2=a_1^2+b_1^2$，

$(a_1,b_1)=1$，$a_1>b_1>0$，$2|a_1$.

由$z^2=a_1^2+b_1^2$得$a_1=2ab$、$b_1=a^2-b^2$、$z=a^2+b^2$、$(a,b)=1$、$a>b>0$、$2|a$，故$x=2a_1b_1=2\cdot 2ab\cdot(a^2-b^2)=4ab(a^2-b^2)$，$y=a_1^2-b_1^2=(2ab)^2-(a^2-b^2)^2=a^4+b^4-6a^2b^2$，$z=a^2+b^2$，并且$(a,b)=1$，$2|a$给出$a+b\equiv 1 \pmod 2$. 所以方程$x^2+y^2=z^4$合条件$x>0$、$y>0$、$z>0$、$(x,y)=1$、$2|x$的解由下式确定：

---

* 原题中$x=4ab(a^2-b^2)$可能有误，因为没有$a>b$这个条件，故要使$x>0$必须取绝对值，即$x=4ab|a^2-b^2|$.

$x=4ab|a^2-b^2|$，$y=|a^4+b^4-6a^2b^2|$，$z=a^2+b^2$，$a>0$，$b>0$，$(a,b)=1$，$a+b\equiv 1 \pmod 2$。

习题 2 证明

$x^4+y^2=z^2$，$2|x$，$y>0$，$z>0$，$(x,y)=1$之解答为

$x=2ab$，$y=|4a^4-b^4|$，$z=4a^4+b^4$，

$(a,b)=1$，$a>0$，$b>0$，$2\nmid b$。

证：合条件的x、y、z可直接验证是方程的解．另一方面，设x、y、z是方程的一组解，且合条件$2|x$、$y>0$、$z>0$、$(x,y)=1$，那么

$x^2=2a_1b_1$，$y=a_1^2-b_1^2$，$z=a_1^2+b_1^2$，

$a_1>b_1>0$，$2|a_1$，$(a_1,b_1)=1$。

由$x^2=2a_1b_1$可得

$a_1=2a^2$，$b_1=b^2$，$(a,b)=1$，$2\nmid b$。

因此，方程$x^4+y^2=z^2$，$2|x$，$y>0$，$z>0$，$(x,y)=1$的解答由下式确定

$x=2ab$，$y=|4a^4-b^4|$，$z=4a^4+b^4$，

$(a,b)=1$，$a>0$，$b>0$，$2\nmid b$。

习题 3 证明不定方程

$$x^2+(x+1)^2=y^2$$

之解为

$$x=\frac{1}{4}\left((1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1}-2\right)$$

$$y=\frac{1}{2\sqrt{2}}\left((1+\sqrt{2})^{2n+1}-(1-\sqrt{2})^{2n+1}\right)$$

且无其他解。

证：设x、y是$x^2+(x+1)^2=y^2$的任一组解。$x^2+(x+1)^2=$

y^2可以变形为

$$(2x+1)^2-2y^2=-1$$

由*Pell*方程熟知的结果，$X_0+Y_0\sqrt{2}=1+\sqrt{2}$是$X^2-2Y^2=-1$的基本解，那么

$$X+Y\sqrt{2}=\pm(1+\sqrt{2})^{2n+1}$$

就是它的全部解．因此

$$(2x+1)^2-2y^2=-1$$

的所有解由下面两式确定

$$(2x+1)+y\sqrt{2}=(1+\sqrt{2})^{2n+1} \qquad (1)$$

$$(2x+1)+y\sqrt{2}=-(1+\sqrt{2})^{2n+1} \qquad (2)$$

由(1)得 $(2x+1)-y\sqrt{2}=(1-\sqrt{2})^{2n+1} \qquad (1')$

把(1)、(1′)联立求解得

$$\begin{cases} x=\dfrac{1}{4}\left((1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1}-2\right) \\ y=\dfrac{1}{2\sqrt{2}}\left((1+\sqrt{2})^{2n+1}-(1-\sqrt{2})^{2n+1}\right) \end{cases} \qquad (3)$$

由(2)得 $(2x+1)-y\sqrt{2}=-(1-\sqrt{2})^{2n+1} \qquad (2')$

把(2)，(2′)联立求解得

$$\begin{cases} x=-\dfrac{1}{4}\left((1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1}+2\right) \\ y=\dfrac{1}{2\sqrt{2}}\left(-(1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1}\right) \end{cases} \qquad (4)$$

把(3)代入原方程的左、右两端：

$$x^2+(x+1)^2=2x^2+2x+1$$

$$=2\left[\frac{1}{4}\left((1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1}-2\right)\right]^2+$$

$$+2\cdot\frac{1}{4}\left((1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1}-2\right)+1$$

$$=\frac{1}{8}\left((1+\sqrt{2})^{4n+2}+(1-\sqrt{2})^{4n+2}+4-2-4(1+\sqrt{2})^{2n+1}-4(1-\sqrt{2})^{2n+1}\right)+\frac{1}{2}\left((1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1}-2\right)+1$$

$$=\frac{1}{8}\left((1+\sqrt{2})^{4n+2}+(1-\sqrt{2})^{4n+2}+2\right);$$

$$y^2=\left[\frac{1}{2\sqrt{2}}\left((1+\sqrt{2})^{2n+1}-(1-\sqrt{2})^{2n+1}\right)\right]^2$$

$$=\frac{1}{8}\left((1+\sqrt{2})^{4n+2}+(1-\sqrt{2})^{4n+2}+2\right).$$

故有　$x^2+(x+1)^2=y^2$

把(4)代入原方程，左、右两端不等。所以

$$x^2+(x+1)^2=y^2$$

的解为　$x=\frac{1}{4}\left((1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1}-2\right)$

$$y=\frac{1}{2\sqrt{2}}\left((1+\sqrt{2})^{2n+1}-(1-\sqrt{2})^{2n+1}\right)$$

且无其他解。

习题 4　关于商高定理$3^2+4^2=5^2$有次之推广：$10^2+11^2+12^2=13^2+14^2$.一般言之，证明

$$(2n^2+n)^2+(2n^2+n+1)^2+\cdots+(2n^2+2n)^2$$
$$=(2n^2+2n+1)^2+\cdots+(2n^2+3n)^2.$$

证： 由平方差公式

$$(2n^2+2n+1)^2-(2n^2+n+1)^2=n(4n^2+3n+2)$$

$$(2n^2+2n+2)^2-(2n^2+n+2)^2=n(4n^2+3n+4)$$

……

$$(2n^2+2n+n)^2-(2n^2+n+n)^2=n(4n^2+3n+2n)$$

把上面诸等式两边分别相加得

$$(2n^2+2n+1)^2-(2n^2+n+1)^2$$

$$+(2n^2+2n+2)^2-(2n^2+n+2)^2+\cdots+$$

$$+(2n^2+3n)^2-(2n^2+2n)^2$$

$$=n(4n^2\cdot n+3n\cdot n+2\cdot\frac{n+1}{2}\cdot n)$$

$$=n(4n^3+4n^2+n)=(2n^2+n)^2.$$

再移项就有

$$(2n^2+n)^2+(2n^2+n+1)^2+\cdots+(2n^2+2n)^2.$$

$$=(2n^2+2n+1)^2+\cdots+(2n^2+3n)^2$$

习题5 求证下列诸曲线上有无穷个有理点:

(a) $\eta^2(d-\xi)=\xi^3$;

(b) $\eta(\xi^2+\eta^2)=d(\eta^2-\xi^2)$;

(c) $\xi^3+\eta^3-3d\xi\eta=0$;

(d) $(\xi^2-d^2)^2-a\eta^2(2\eta+3d)=0$.

证: (a) 考虑合条件 $(a,b)=1$、$\sqrt{ad-b}$ 非有理数的二次曲线

$$b^3x^2-a^2(ad-b)y^2=0$$

设
$$S(x,y)=b^3x^2-a^2(ad-b)y^2$$

显然，$S(x,y)=0$ 在有理数域上不会退化成直线且有有理系数，还经过坐标原点. 故由定理9可知，二次曲线 $S(x,y)=0$ 上有无穷多个有理点 $(x,y)=\left(\frac{\beta}{a},\ \frac{s}{r}\right)$，$\beta s\neq 0$. 也就是说，有无穷多组 $\left(\frac{\beta}{a},\ \frac{s}{r}\right)$ 使下式成立

$$b^3\left(\frac{\beta}{a}\right)^2-a^2(ad-b)\left(\frac{s}{r}\right)^2=0$$

两端同除以$a^3\left(\frac{\beta}{a}\right)^2$得

$$\left(\frac{b}{a}\right)^3-\frac{ad-b}{a}\left(\frac{\alpha s}{r\beta}\right)^2=0$$

$$\left(\frac{\alpha s}{r\beta}\right)^2\left(d-\frac{b}{a}\right)=\left(\frac{b}{a}\right)^3$$

令$\xi=\frac{b}{a}$、$\eta=\frac{\alpha s}{r\beta}$，上式变为

$$\eta^2(d-\xi)=\xi^3$$

此即曲线$\eta^2(d-\xi)=\xi^3$上有无穷多个有理点

$$(\xi,\eta)=\left(\frac{b}{a},\ \frac{\alpha s}{r\beta}\right)$$

(b) 考虑合条件$m\neq 0$、$\sqrt{dm-n}$非有理数的二次曲线

$$n^2(n-dm)x^2+m^2(n+dm)y^2=0$$

设 $P(x,y)=n^2(n-dm)x^2+m^2(n+dm)y^2$

显然$P(x,y)=0$在有理数域上不会退化成直线且有有理系数，还经过坐标原点。故由定理 9 可知，二次曲线$P(x,y)=0$上有无穷多个有理点$(x,y)=\left(\frac{\beta}{a},\ \frac{s}{r}\right)$、$\beta s\neq 0$，也就是说，有无穷多组$\left(\frac{\beta}{a},\ \frac{s}{r}\right)$使下式成立

$$n^2(n-dm)\left(\frac{\beta}{a}\right)^2+m^2(n+dm)\left(\frac{s}{r}\right)^2=0$$

上式两端同除以$m^3\left(\frac{\beta}{a}\right)^2$得

$$\left(\frac{n}{m}\right)^3-\left(\frac{n}{m}\right)^2d+\left(\frac{n}{m}+d\right)\left(\frac{\alpha s}{r\beta}\right)^2=0$$

$$\frac{n}{m}\left[\left(\frac{as}{r\beta}\right)^2+\left(\frac{n}{m}\right)^2\right]=d\left[\left(\frac{n}{m}\right)^2-\left(\frac{as}{r\beta}\right)^2\right]$$

命$\xi=\frac{as}{r\beta}$、$\eta=\frac{n}{m}$，上式变为

$$\eta(\xi^2+\eta^2)=d(\eta^2-\xi^2)$$

即曲线$\eta(\xi^2+\eta^2)=d(\eta^2-\xi^2)$上有无穷多个有理点

$$(\xi,\eta)=\left(\frac{as}{r\beta},\ \frac{n}{m}\right).$$

(*c*) 对合条件$b+n\neq 0$、$b\cdot n\neq 0$的任意整数b、n，设

$$\frac{b^3+n^3}{3dbn}=\frac{s}{r}$$

即
$$b^3+n^3-3dbn\frac{s}{r}=0$$

上式两端同除以$\left(\frac{s}{r}\right)^3$得

$$\left(\frac{rb}{s}\right)^3+\left(\frac{rn}{s}\right)^3-3d\left(\frac{rb}{s}\right)\left(\frac{rn}{s}\right)=0$$

命$\xi=\frac{rb}{s}$、$\eta=\frac{rn}{s}$，则

$$\xi^3+\eta^3-3d\xi\eta=0$$

再由合条件$b\neq -n$、$bn\neq 0$的整数b、n有无穷多对可知，曲线

$$\xi^3+\eta^3-3d\xi\eta=0$$

上有无穷多个有理点.

(*d*) 显然$a\neq 0$.

设
$$\eta=\frac{k^2-3ad}{2a} \tag{1}$$

原方程变形为

$$(\xi^2-d^2)^2=k^2\eta^2$$

从而 $$\xi^2=\frac{k^3}{2a}-\frac{3dk}{2}+d^2 \qquad (2)$$

或 $$\xi^2=\frac{-k^3}{2a}+\frac{3dk}{2}+d^2 \qquad (3)$$

若能证明曲线(2)或(3)上有无穷多个有理点 (ξ,k),那么由(1)便知曲线

$$(\xi^2-d^2)^2-a\eta^2(2\eta+3d)=0$$

上有无穷多个有理点 $(\xi,\ \eta)$. 下面证明曲线(2)上有无穷多个有理点. 用同法可证曲线(3)上也有无穷多个有理点.

考虑二次曲线

$$Q(x,y)=2a\alpha^3x^2+(3ad\alpha^2b-2ad^3\alpha^3-b^3)y^2=0$$

其中α、b为有理数,且使$Q(x,y)=0$在有理数域内不退化成直线。显然,$Q(x,y)=0$ 经过坐标原点. 由定理 9 知道曲线$Q(x,y)=0$上有无穷多个有理点$(x,y)=\left(\frac{s}{r},\ \frac{\delta}{\beta}\right)$,$s\delta\neq 0$,即有无穷多个有理点$\left(\frac{s}{r},\ \frac{\delta}{\beta}\right)$,且满足下式

$$2a\alpha^3\left(\frac{s}{r}\right)^2+(3ad\alpha^2b-2ad^2\alpha^3-b^3)\left(\frac{\delta}{\beta}\right)^2=0$$

由于$Q(x,y)=0$ 非退化,故有$\alpha\neq 0$,上式两端同除以$\alpha^3\left(\frac{\delta}{\beta}\right)^2$得

$$2a\left(\frac{s\beta}{r\delta}\right)^2+3ad\left(\frac{b}{\alpha}\right)-2ad^2-\left(\frac{b}{\alpha}\right)^3=0$$

命$\xi=\frac{s\beta}{r\delta}$、$k=\frac{b}{\alpha}$得

$$2a\xi^2=k^3-3adk-2ad^2$$

即曲线
$$\xi^2=\frac{k^3}{2a}-\frac{3dk}{2}+d^2$$
上有无穷多个有理点。

习题 6 定出所有的三角形，其边及面积皆为有理数者。

解：用x、y、z、w分别表三角形的三条边长及面积，则由“Helon—秦九韶”三斜求积公式

$$w=\sqrt{s(s-x)(s-y)(s-z)}$$

$$s=\frac{1}{2}(x+y+z)$$

得
$$(4w)^2+(x^2-y^2+z^2)^2=(2xz) \qquad (1)$$
i) 首先证明在钝角和锐角三角形类中，不存在边长及面积都是有理数的三角形。不妨设x、y、z都是正整数，否则可用它们分母的最小公倍数去与它们相乘，就得一个以正整数mx、my、mz为边长的三角形。由相似性质可知，此三角形的面积是原三角形面积的m^2倍，从而要证以有理数x、y、z为边长的三角形的面积为有理数，须且只须证明以正整数mx、my、mz为边长的三角形的面积为有理数即可。

如果w为有理数，由x、y、z为正整数，结合（1）可知$4w$为正整数。又因为
$$x^2-y^2+z^2\neq 0$$
故由（1）可得
$$\begin{cases}4w=2dab\\ x^2-y^2+z^2=d(b^2-a^2)\\ 2xz=d(b^2+a^2)\end{cases}$$

或
$$\begin{cases}4w=d(b^2-a^2)\\ x^2-y^2+z^2=2dab\\ 2xz=d(b^2+a^2)\end{cases}$$

其中d为正整数，且a、b合条件

$$b>a>0,\quad (a,b)=1,\quad a+b\equiv 1\ (\mathrm{mod}2)\text{ . 所以}$$

$$y^2=x^2+z^2-d(b^2-a^2)$$

$$=x^2+z^2-d(b^2-a^2)\frac{2xz}{d(b^2+a^2)}$$

$$=x^2+z^2-\frac{2(b^2-a^2)}{b^2+a^2}xz$$

或
$$y^2=x^2+z^2-2dab$$

$$=x^2+z^2-2dab\frac{2xz}{d(b^2+a^2)}$$

$$=x^2+z^2-\frac{4ab}{b^2+a^2}xz.$$

由余弦定理得

$$\cos\theta_{xz}=\frac{b^2-a^2}{b^2+a^2}$$

或
$$\cos\theta_{xz}=\frac{2ab}{b^2+a^2}.$$

其中θ_{xz}表示以边长为x、z的两条边所夹的角。此二式均给出

$$0<\cos\theta_{xz}<1$$

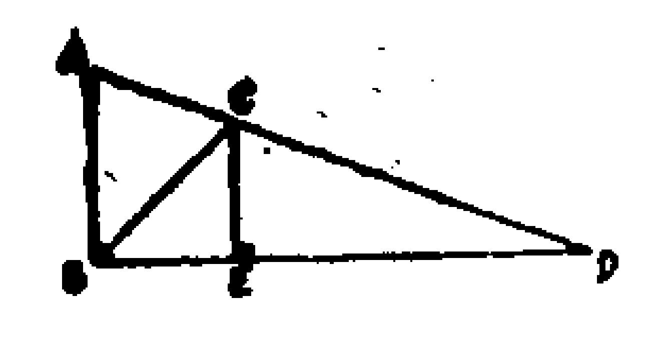
用完全相同的方法可以证明

$$0<\cos\theta_{xy}<1,\quad 0<\cos\theta_{yz}<1.$$

这样就证明了以正整数x、y、z为边长的非直角三角形如果面积为有理数，则它一定是锐角三角形。也就是说，在钝角三角形类中，不存在边长和面积都是有理数的三角形。

在锐角三角形类中，如果存在一个$\triangle ABC$，它的边长和面积都是有理数，则由前证可知它的三个内角的正弦、余弦、正切、余切都是有理数。我们可过顶点B作AB的垂线，使其与AC边的延长线相交于D，便得直角$\triangle ABD$。再设CE为$\triangle BCD$的边BD上

的高，如右下图所示：



利用$\triangle ABC$的三条边及三内角的三角函数都是有理数，容易推出BC、CD、DB及CE全都是有理数，因此$\triangle BCD$的各边及面积都是有理数．但$\triangle BCD$是钝角三角形，此与前证矛盾．所以，在锐角三角形类中，各边及面积都是有理数的三角形，也是不存在的．

ii）因为直角三角形各边及面积都是有理数，与各边是有理数等价，所以直角三角形类中，各边及面积都是有理数的三角形的三条边，由不定方程

$$x^2+z^2=y^2 \qquad (2)$$

的正有理数解给出．下面证明（2）的全体正有理数解可表为

$$\begin{cases} x=\dfrac{2Dab}{n} \\ z=\dfrac{D(b^2-a^2)}{n} \\ y=\dfrac{D(b^2+a^2)}{n} \end{cases} \qquad 〈\text{I}〉$$

或

$$\begin{cases} x=\dfrac{D(b^2-a^2)}{n} \\ z=\dfrac{2Dab}{n} \\ y=\dfrac{D(b^2+a^2)}{n} \end{cases} \qquad (\text{II})$$

其中D、n为任意正整数，a、b是满足条件

$b>a$，$(a,b)=1$，$a+b\equiv 1 \pmod 2$

的任意正整数．可直接验证〈I〉、〈II〉是（2）的解．另一方面，设

$$x=\frac{y_1}{x_1},\quad y=\frac{y_2}{x_2},\quad z=\frac{y_3}{x_3}$$

是(2)的一组既约正有理数解，x_i、y_i，$(1\leqslant i\leqslant 3)$ 都是正整数。设$n=[x_1, x_2, x_3]$，由(2)得

$$\left(n\frac{y_1}{x_1}\right)^2+\left(n\frac{y_3}{x_3}\right)^2=\left(n\frac{y_2}{x_2}\right)^2$$

再设 $\left(n\frac{y_1}{x_1},n\frac{y_3}{x_3}\right)=D$, $n\frac{y_1}{x_1}=DX$,

$$n\frac{y_3}{x_3}=DZ,\quad n\frac{y_2}{x_2}=DY$$

就有

$$X^2+Z^2=Y^2$$

故有

$$\begin{cases}X=2ab\\Z=b^2-a^2\\Y=b^2+a^2\end{cases}$$

或

$$\begin{cases}X=b^2-a^2\\Z=2ab\\Y=b^2+a^2\end{cases}$$

其中a、b合条件

$b>a>0$，$(a, b)=1$，$a+b\equiv 1(\bmod 2)$．

即

$$\begin{cases}\dfrac{y_1}{x_1}=\dfrac{2Dab}{n}\\[2ex]\dfrac{y_3}{x_3}=\dfrac{D(b^2-a^2)}{n}\\[2ex]\dfrac{y_2}{x_2}=\dfrac{D(b^2+a^2)}{n}\end{cases}$$

或

$$\begin{cases}\dfrac{y_1}{x_1}=\dfrac{D(b^2-a^2)}{n}\\[2ex]\dfrac{y_3}{x_3}=\dfrac{2Dab}{n}\\[2ex]\dfrac{y_2}{x_2}=\dfrac{D(b^2+a^2)}{n}\end{cases}$$

这就证明了不定方程（2）的任意一组正有理数解可由〈Ⅰ〉或〈Ⅱ〉表出。

由i）、ii）可知，各边及面积都是有理数的三角形，只能在直角三角形类中找到，它们由〈Ⅰ〉或〈Ⅱ〉给出。

习题7 研究不定方程

$$x^2+y^2+z^2=w^2 \qquad (A)$$

之解。

解：下面证明不定方程

$$x^2+y^2+z^2=w^2$$

的解由下式给出：*

$$dx=2X_1X_3,\quad dy=2X_2X_3,$$
$$dz=X_3^2-X_2^2-X_1^2,\quad dw=X_3^2+X_2^2+X_1^2 \qquad (1)$$

其中d、X_i，（$1\leqslant i\leqslant 3$）为任意整数。

因为 $d^2x^2+d^2y^2+d^2z^2$

$$=(2X_1X_3)^2+(2X_2X_3)^2+(X_3^2-X_2^2-X_1^2)^2$$
$$=4X_1^2X_3^2+4X_2^2X_3^2+X_3^4+X_2^4+X_1^4-2X_3^2X_2^2-2X_3^2X_1^2+2X_2^2X_1^2$$
$$=X_3^4+X_2^4+X_1^4+2X_3^2X_2^2+2X_3^2X_1^2+2X_2^2X_1^2$$
$$=(X_3^2+X_2^2+X_1^2)^2=d^2w^2$$

上式两端约去d^2得

$$x^2+y^2+z^2=w^2$$

此即合条件（1）的x、y、z、w是(A)的解。设x、y、z、w是(A)的任一组解。命

---

* 用相同的方法可以推出不定方程$x_1^2+x_2^2+\cdots+x_n^2=x^2$的解，由下式给出：

$$dx_r=2X_rX_n,\quad (r=1,\ 2,\ \cdots,\ n-1)$$
$$dx_n=X_n^2-X_1^2-\cdots-X_{n-1}^2$$
$$dx=X_n^2+X_1^2+\cdots+X_{n-1}^2$$

其中d、X_i（$1\leqslant i\leqslant n$）为任意整数。

$$x=X_1,\quad y=X_2,\quad z=Z_3-w \tag{2}$$

就有 $X_1{}^2+X_2{}^2+(X_3-w)^2=w^2$

即
$$X_1{}^2+X_2{}^2+X_3{}^2=2wX_3 \tag{3}$$

同样，由(2)还有
$$X_3{}^2-X_2{}^2-X_1{}^2=2zX_3 \tag{4}$$

(2)、(3)、(4)给出
$$\frac{x}{2X_1X_3}=\frac{y}{2X_2X_3}=\frac{z}{X_3{}^2-X_2{}^2-X_1{}^2}=\frac{w}{X_3{}^2+X_2{}^2+X_1{}^2}$$
$$=\frac{1}{2X_3} \tag{5}$$

取$d=2X_3$，由(5)得
$$dx=2X_1X_3,\quad dy=2X_2X_3,$$
$$dz=X_3{}^2-X_2{}^2-X_1{}^2,\quad dw=X_3{}^2+X_2{}^2+X_1{}^2$$

这就证明了$x^2+y^2+z^2=w^2$的解合条件(1)。所以，不定方程$x^2+y^2+z^2=w^2$的解由(1)给出。

习题8 设整数a、b、c不同号，$abc\neq 0$，且abc无平方因子，则不定方程
$$ax^2+by^2+cz^2=0$$
有不全为零的整数解的充要条件是：$-bc$是a的二次剩余，$-ac$是b的二次剩余，$-ab$是c的二次剩余。

证：设$a>0$，$b>0$，$c<0$，$-c=c_1$，原方程变为
$$ax^2+by^2=c_1z^2$$
不失一般，可假定$(a,b,c_1)=1$，而且还可进一步假定$(a,b)=(a,c_1)=(b,c_1)=1$。因为如果$(a,b)=d$，$(a,c_1)=e$，$(b,c_1)=f$，则由$(a,b,c_1)=1$，可得$(d,e)=(d,f)=(e,f)=1$，且a、b、c_1无平方因子可得$d|z$，$e|y$，$f|x$。于是可设$a=dea_1$，$b=dfb_1$，$c_1=efc_2$，$x=fx_1$，$y=ey_1$，$z=dz_1$，方程$ax^2+by^2=c_1z^2$变为
$$a_1fx_1{}^2+b_1ey_1{}^2=c_2dz_1{}^2$$

其中 $(a_1f, b_1e)=(a_1f,c_2d)=(b_1e,c_2d)=1$

下面证明$ax^2+by^2=c_1z^2$有不全为零的整数解x、y、z，且由$(x,y,z)=1$的充要条件是

$$\left(\frac{-ab}{c_1}\right)=\left(\frac{bc_1}{a}\right)=\left(\frac{ac_1}{b}\right)=1$$

从而本题结论也就被证明了.

先证必要性．设$ax^2+by^2=c_1z^2$有一组不全为0的解x、y、z，且$(x,y,z)=1$．显然，x、y不能都为零，且$z\neq 0$．设$x=0$，$y\neq 0$，则$c_1|by^2$．又因$(c_1, b)=1$，故$c_1|y^2$．现证$c_1=1$．若$c_1>1$，则有素数$p|c_1$、$p|y^2$推出$p^2|c_1z^2$．因c_1无平方因子，所以$p|z$，与$(z,y)=1$矛盾，故$c_1=1$，显然$\left(\frac{-ab}{c_1}\right)=1$．

同样可证$x\neq 0$、$y=0$的情况．再设$x\neq 0$、$y\neq 0$，由$ax^2+by^2\equiv 0 \pmod{c_1}$及$(aby^2, c_1)=1$可得$ax^2\equiv -by^2 \pmod{c_1}$、$(ax)^2\equiv -aby^2 \pmod{c_1}$，从而得到

$$\left(\frac{-aby^2}{c_1}\right)=\left(\frac{-ab}{c_1}\right)=1$$

同理可证 $$\left(\frac{bc_1}{a}\right)=\left(\frac{ac_1}{b}\right)=1$$

再证充分性．当$a=b=c_1=1$时，方程

$$ax^2+by^2=c_1z^2$$

显然有不全为零的解，以下除去这一情形．因$\left(\frac{-ab}{c_1}\right)=1$，$(a,c_1)=1$，故有整数$k$，使得$k^2\equiv -ab \pmod{c_1}$及存在整数$a'$，使得$aa'\equiv 1 \pmod{c_1}$，于是得

$ax^2+by^2-c_1z^2\equiv ax^2+by^2\equiv a'a^2x^2+a'aby^2\equiv a'(a^2x^2-k^2y^2)\equiv a'(ax-ky)(ax+ky) \pmod{c_1}$因为$\left(\frac{bc_1}{a}\right)=\left(\frac{ac_1}{b}\right)=$

1，$(a,b)=1$，故存在整数s、t，使$s^2\equiv bc_1(\bmod a)$，$t^2\equiv ac_1(\bmod b)$及存在整数b'和a''，使$bb'\equiv 1(\bmod a)$，$aa''\equiv 1(\bmod b)$，因而有

$$ax^2+by^2-c_1z^2\equiv ax^2-c_1z^2\equiv a''a^2x^2-a''ac_1z^2$$

$$\equiv a''(ax-tz)(ax+tz)(\bmod b)$$

$$ax^2+by^2-c_1z^2\equiv by^2-c_1z^2\equiv b'b^2y^2-b'bc_1z^2$$

$$\equiv b'(by-sz)(by+sz)(\bmod a)$$

总之，存在

$$L_j(x,y,z)=l_jx+m_jy+n_jz,$$

$$M_j(x,y,z)=u_jx+v_jy+w_jz,$$

$$j=1,\ 2,\ 3.$$

使得

$$ax^2+by^2-c_1z^2\equiv L_1(x,y,z)M_1(x,y,z)(\bmod a)$$

$$ax^2+by^2-c_1z^2\equiv L_2(x,y,z)M_2(x,y,z)(\bmod b)$$

$$ax^2+by^2-c_1z^2\equiv L_3(x,y,z)M_3(x,y,z)(\bmod c_1)$$

由孙子定理，存在整数l、m、n和u、v、w，满足：

$l\equiv l_1(\bmod a)$，$l\equiv l_2(\bmod b)$，$l\equiv l_3(\bmod c_1)$，

$m\equiv m_1(\bmod a)$，$m\equiv m_2(\bmod b)$，$m\equiv m_3(\bmod c_1)$，

$n\equiv n_1(\bmod a)$，$n\equiv n_2(\bmod b)$，$n\equiv n_3(\bmod c_1)$，

$u\equiv u_1(\bmod a)$，$u\equiv u_2(\bmod b)$，$u\equiv u_3(\bmod c_1)$，

$v\equiv v_1(\bmod a)$，$v\equiv v_2(\bmod b)$，$v\equiv v_3(\bmod c_1)$，

$w\equiv w_1(\bmod a)$，$w\equiv w_2(\bmod b)$，$w\equiv w_3(\bmod c_1)$.

设
$$L(x,y,z)=lx+my+nz$$

$$M(x,y,z)=ux+vy+wz$$

则有 $ax^2+by^2-c_1z^2\equiv L(x,y,z)M(x,y,z)(\bmod abc_1)$

考虑整数组成的三元有序集：

$$T=\{(x,y,z)\mid 0\leqslant x<\sqrt{bc_1},\ 0\leqslant y<\sqrt{ac_1},\ 0\leqslant z<\sqrt{ab}\}$$

注意到$\sqrt{bc_1}$、$\sqrt{ac_1}$、$\sqrt{ab}$都是无理数，从而x、y、z分别在T中可取$[\sqrt{bc_1}]+1$、$[\sqrt{ac_1}]+1$、$[\sqrt{ab}]+1$个值。由此推出T中元素个数等于

$([\sqrt{ab_1}]+1)([\sqrt{ac_1}]+1)([\sqrt{ab}]+1)>\sqrt{lc_1}\cdot\sqrt{ac_1}\cdot\sqrt{ab}=abc_1$

于是在T中至少有两个不同元素(x_1,y_1,z_1)和(x_2,y_2,z_2)使得

$$L(x_1,y_1,z_1)\equiv L(x_2,y_2,z_2)\pmod{abc_1}$$

因此　$L(x_1-x_2,y_1-y_2,z_1-z_2)\equiv 0\pmod{abc_1}$

设　$|x_1-x_2|=x$，$|y_1-y_2|=y$，$|z_1-z_2|=z$

即有一组不全为零的解，使得

$$ax^2+by^2-c_1z^2\equiv 0\pmod{abc_1}$$

成立，并且

$$0\leqslant x<\sqrt{bc_1}\ ,\ 0\leqslant y<\sqrt{ac_1}\ ,\ 0\leqslant z<\sqrt{ab}$$

从而　$-abc_1<ax^2+by^2-c_1z^2<2abc_1$

故得　$ax^2+by^2-c_1z^2=0$

或　$ax^2+by^2-c_1z^2=abc_1$

由$ax^2+by^2-c_1z^2=abc_1$有

$$(ax^2+by^2)(z^2+ab)=c_1(z^2+ab)^2$$

即　$a(xz+by)^2+b(yz-ax)^2=c_1(z^2+ab)^2$

令　$xz+by=X$，$yz-ax=Y$，$z^2+ab=Z\neq 0$

于是　$aX^2+bY^2=c_1Z^2$

总之，可以得到一组不全为零的解。约去它们的最大公因数可得

$$ax^2+by^2=c_1z^2$$

的一组解x、y、z，合条件$(x,y,z)=1$。

下面对此题再给出一个证明。用(1)、(2)，(3)、(4)分别表示

(1)系数两两互素，不同号，无一为零；

（2）abc无平方因子>1；

（3）$ax^2+by^2+cz^2=0$有不全为零的整解；

（4）$-bc$、$-ca$、$-ab$依次为a、b、c的平方剩余。

不失一般，可设a、b、c两两互素。

Ⅰ　设（3）有不全为零的整解，约去公因子，可得一个公因子为1的解x、y、z。如素数$p|(x,y)$，有$p^2|cz^2$；但$p^2\nmid c$，故$p|z$；因$(x,y,z)=1$，故$(x,y)=1$，可设x、y、z两两互素。

因此，$(a,z)=1$．由于$p|(a,z)$，则$p|by^2$和$(a,b)=(y,z)=1$矛盾，故$zw\equiv 1 \pmod{a}$ 有解w，乘（3）以bw^2得出$-bc\equiv (byw)^2 \pmod{a}$．同理可证（4）的其余部分。

Ⅱ　设（1）、（2）、（4）成立，来证明（3）可解。如果正整数

$$|bc|,\ |ca|,\ |ab| \qquad (5)$$

均不同，定义（3）的指标为此三数的中间数(依大小计)。如在(5)中有二数相同或三数相同，则定义指标为此相同的数。

当指标为1时，（5）中至少有一数为1，设$|ab|=1$，则(5)为$|c|$、$|c|$、1．按定义$|c|=1$，因a、b、c不全同号，可取$a=1$、$b=-1$，故（3）有解$x=y=1$，$z=0$，这对指标为1证明了习题。

用归纳法。设对指标$<J$时，习题已经证明，来证明对指标为J时亦成立，从而证明（3）有指标$J\geq 2$．由对称性可设

$$|a|\leq|b|\leq|c| \qquad (6)$$

于是$|ab|\leq|ac|\leq|bc|$，而$J=|ac|$．因$(b,c)=1$，从$|b|=|c|$将推出$|b|=|c|=1$．由（6）得$|a|=1$，从而$J=1$，和$J\geq 2$矛盾。故有

$$|a|\leq|b|<|c|,\quad |ab|<|ac|=J\leq|bc| \qquad (7)$$

由（4），$an^2\equiv -b \pmod{c}$ 有解n，使得$|n|\leq\frac{1}{2}|c|$，故有

$$an^2+b=cQ \tag{8}$$

$$|Q|\leqslant\frac{|a|n^2+|b|}{|c|}\leqslant\frac{1}{4}|ac|+\left|\frac{b}{c}\right|<\frac{1}{4}J+1<J \tag{9}$$

$Q=0$ 的情形可除外，因$(b,c)=1$且无平方因子．$b=-an^2$将给出$|n|=1$、$b=-a=\pm1$，从而(3)有解$x=y=1$、$z=0$.

我们将把(3)化为有较小指标的同形方程．设(8)的三项的$g.c.d$为A，从而A为此三项的任二项的$g.c.d$．因$A|b$，故$(A,ac)=1$．由此，$A|n^2$，$A|Q$．但b的因子A无平方因子>1，故$A|n$．可写出

$$n=A\alpha,\ b=A\beta,\ Q=Ag=ACr^2 \tag{10}$$

其中r^2是g中最大的平方因子．于是，(8)给出

$$aA\alpha^2+\beta=cCr^2 \tag{11}$$

其三项两两互素，写$B=a\beta$．现在来证明

$$AX^2+BY^2+CZ^2=0 \tag{12}$$

有性质(1)和(2)，以及

$-BC$、$-CA$、$-AB$依次为A、B、C的平方剩余 (13)

显然，A、B、C无一为零．因$(a,b)=1$，且无一有平方因子>1，由$AB=ab$推出A和B均无平方因子>1，而且$(A,B)=1$．因r^2是$g=Cr^2$的最大平方因子，故C无平方因子>1．因(11)的各项两两互素，故C和$aA\beta=AB$互素．

其次，A、B、C不全同号，这在$ab=AB<0$时成立，故设$ab>0$．因(1)、ca和bc均为负数，故由

$$c(an^2+b)=c^2Q=c^2ACr^2$$

推出$AC<0$．这就证明了(12)有性质(1)和(2)．

由(11)，其各项两两互素，可知βcC，$acAC$和$-aA\beta=-AB$依次为aA、β、C的平方剩余．现在只须证明(13)的前面部分．由(4)，$-bc=-\beta Ac$和$-ca$依次是a和$b=A\beta$的平方剩余，因βcC和$-ca$是A的平方剩余，其乘积为$-BCc^2$，从而$-BC$亦是A的平方

剩余．因 $-ca$ 和 $acAC$ 是 β 的平方剩余，$-AC\equiv u^2 \pmod{\beta}$ 有解 u；βcC 和 $-\beta Ac$ 是 a 的平方剩余，从而 $-AC\equiv v^2 \pmod{a}$ 有解 v．由(11)知 $(a,\beta)=1$，故有解 $w\equiv u \pmod{\beta}$，$w\equiv v \pmod{a}$，于是 $AC+w^2$ 可被 β 和 a 除尽，亦即被 $\beta a=B$ 除尽，这就证明了(13)．由(7)、(9)和(10)有：

$$|AB| = |ab| < J,\quad |CA| \leqslant CA|r^2 = |Q| < J$$

故(12)的指标 $<J$．由假设，(12)有整数解 X、Y、Z 不全为零，取

$$x = A\alpha X - \beta Y,\quad y = X + a\alpha Y,\quad z = CrZ$$

则由(10)、(11)和 $B=a\beta$，得出

$$ax^2+by^2+cz^2 = cCr^2(AX^2+BY^2+CZ^2) = 0$$

如 $x=y=0$，消去 X，给出 $(\beta + Aa\alpha^2)Y=0$．由(11)，前一因子不为零，故 $Y=0$，$X=0$，从而 $Z=0$，与假设矛盾．这就完成了我们的全部证明．

本题的第二种证法，由柯召教授给出．

§ 7 Fermat猜测

习题 1 证明次诸不定方程无解：

(a) $x^4+4y^4=z^2$，$x>0$，$y>0$；

(b) $x^4-y^4=z^2$，$y>0$，$z>0$；

(c) $x^4-y^4=2z^2$，$y>0$，$z>0$，

(d) $x^4-y^4=pz^2$，$z>0$．

此处 p 为素数，$p\equiv 3 \pmod{8}$．

证： (a) 设 $z=u$ 是使(a)成立的最小正整数解，显然 $(x,y)=1$，否则 $\dfrac{u}{(x,y)^2}$ 也是解，此与 u 最小矛盾．因此，x、y 不全为偶数．如果 x 和 y 都是奇数，则 $x^4+4y^4=u^2$ 给出 $5\equiv 1 \pmod{8}$，此不可

能。如果x为偶数，y为奇数，设$x=2x_1$，就有$4x_1^4+y^4=\left(\frac{u}{2}\right)^2$，

$\frac{u}{2}<u$，也与u最小矛盾。如x为正奇数，y为偶数，就有$(x^2, 2y^2)=1$，$x^4+4y^4=u^2$给出$x^2=a^2-b^2$，$y^2=ab$，$u=a^2+b^2$，$(a,b)=1$，$a>b>0$，且a奇b偶，因若a偶就有$x^2\equiv-1\pmod 4$。设$b=2c$，$y^2=ab=2ac$，$a=d^2$，$c=2f^2$，$x^2=a^2-b^2=(d^2)^2-(4f^2)^2$。同理，$(4f^2,x)=1$，$4f^2=2lm$，$x=l^2-m^2$，$d^2=l^2+m^2$，$l>m>0$，$(l, m)=1$。不妨设$l$奇，$m$偶，由$2f^2=lm$有$l=r^2$，$m=2s^2$，$d^2=l^2+m^2=(r^2)^2+(2s^2)^2=r^4+4s^4$，即$r$、$s$、$d$也是方程$(a)$的一组解，且$d<d^2=a<a^2+b^2=u$，此仍与$u$最小矛盾。

(b)如果$x^4-y^4=z^2$有解x_0、y_0、z_0，不妨设$x_0>0$，$y_0>0$，$z_0>0$，则由$x_0^4-y_0^4=z_0^2$有$(x_0^4-y_0^4)^2=(z_0^2)^2$，$z_0^4+4(x_0y_0)^4=(x_0^4+y_0^4)^2$，即$z_0$、$x_0y_0$、$x_0^4+y_0^4$是方程$(a)$的一组解，此与$(a)$无解矛盾。

(c)设$z=u$是使$x^4-y^4=2z^2$、$y>0$、$z>0$成立的最小正整数，下面证明$(x,y)=1$。若$(x,y)=d$，$q\neq 2$是d的一个素因子，则$q^2|u$，$\frac{u}{q^2}$也是解，而$\frac{u}{q^2}<u$，与u最小矛盾。因此，$d=2$或者1。

而当$d=2$时，设$x=2x_1$，$y=2y_1$，就有$2^4(x_1^4-y_1^4)=2u^2$，$x_1^4-y_1^4=\frac{u^2}{2^3}=2\left(\frac{u}{2^2}\right)^2$，从而，$\frac{u}{2^2}$也是解，这也与$u$最小矛盾，

因此，$(x,y)=1$，且x、y同奇。此时，u一定是偶数，否则，$x^4-y^4=2u^2$给出$0\equiv2\pmod 4$。因此，$(x^2+y^2, x^2-y^2)=2$。由$x^4-y^4=(x^2+y^2)(x^2-y^2)=2u^2$有

$$\begin{cases}x^2+y^2=4a^2\\x^2-y^2=2b^2\end{cases}$$

或
$$\begin{cases} x^2+y^2=2b^2 \\ x^2-y^2=4a^2 \end{cases}$$

其中 $(a,b)=1$，$u=2ab$，$a>0$，$b>0$。

但是$x^2+y^2=4a^2$给出 $2\equiv 0 \pmod 4$，而$x^2-y^2=4a^2$给出$x=s^2+t^2$，$y=s^2-t^2$，$a=st$，$(s,t)=1$，$s>t>0$，再由$x^2+y^2=2b^2$就有$s^4+t^4=b^2$，此不可能。

(d)设$z=u$是最小正整数解，则必有 $(x,y)=1$。设$(x,y)=d$，$q\neq p$是d的任一素因子，则$q^4|u^2$，$q^2|u$，$\dfrac{u}{q^2}$也是方程的解，与u最小矛盾。因此，$d=p$或者1。若$d=p$，设$x=px_1$，$y=py_1$，则$p^4(x_1{}^4-y_1{}^4)=pu^2$，$p^3|u^2$，$p^2|u$，$\dfrac{u}{p^2}$也是解，此亦不可能，故 $(x,y)=1$。

i) 如果x偶y奇，$x^4-y^4=pu^2$给出$-1\equiv p\equiv 3 \pmod 8$，矛盾。

ii) 如果x奇y偶，则有 $(x^2+y^2, x^2-y^2)=1$，$x^4-y^4=pu^2$给出
$$\begin{cases} x^2+y^2=pa^2 \\ x^2-y^2=b^2 \end{cases}$$
或
$$\begin{cases} x^2+y^2=b^2 \\ x^2-y^3=pa^2 \end{cases}$$
其中$u=ab$，$(a,b)=1$。

但是，$x^2+y^2=pa^2$和$x^2-y^2=pa^2$均给出$1\equiv p \pmod 4$，与$p\equiv 3 \pmod 8$矛盾。

iii) 如果x奇y奇，此时$(x^2+y^2, x^2-y^2)=2$，$x^4-y^4=pu^2$给出
$$\begin{cases} x^2+y^2=2pa^2 \\ x^2-y^2=2b^2 \end{cases} \qquad (\text{I})$$

或 $$\begin{cases}x^2+y^2=2b^2\\x^2-y^2=2pa^2\end{cases}\qquad(\text{Ⅱ})$$

其中$u=2ab$，$(a,b)=1$．如果（Ⅰ）成立，定有a奇b偶，则$x^2=pa^2+b^2$给出$1\equiv p(\bmod 4)$，此与$p\equiv3(\bmod 8)$矛盾；如果（Ⅱ）成立，定有a偶b奇．设

$x=X+Y$，$y=X-Y$，$(X, Y)=1$，则$x^2+y^2=2b^2$就变为
$$X^2+Y^2=b^2$$

不妨设$b>0$，$X>0$，$Y>0$，$2|X$，则

$X=2cd$，$Y=c^2-d^2$，$b=c^2+d^2$，$c>d>0$，$(c,d)=1,c+d\equiv1(\bmod 2)$

再不妨设$2|c$，从而有
$$\begin{cases}x=X+Y=2cd+(c^2-d^2)\\y=X-Y=2cd-(c^2-d^2)\end{cases}\qquad(1)$$

对于$x^2-y^2=2pa^2$，设$a=2^ta_1$，$2\nmid a_1$，$t\geqslant1$，则$x^2-y^2=2^{2t+1}pa_1^2$给出
$$\begin{cases}x+y=2^{2t}pb_1^2\\x-y=2c_1^2\end{cases}\qquad(2)$$

或 $$\begin{cases}x+y=2c_1^2\\x-y=2^{2t}pb_1^2\end{cases}\qquad(3)$$

或 $$\begin{cases}x+y=2^{2t}b_1^2\\x-y=2pc_1^2\end{cases}\qquad(4)$$

或 $$\begin{cases}x+y=2pc_1^2\\x-y=2^{2t}b_1^2\end{cases}\qquad(5)$$

其中$a_1=b_1c_1$，$(b_1, c_1)=1$，$b_1>0$，$c_1>0$．(1)和(2)给出$c^2=c_1^2+d^2$，但c偶、c_1奇，d也奇，故不可能；(1)和(3)给出$c_1^2=2cd$，由c_1奇知亦不可能；(1)和(5)给出$pc_1^2=2cd$，由p、c_1均为奇知仍然不可能；最后，由(1)和(4)得出$4cd=2^{2t}b_1^2$，从而cd为一完全平方数；又因为$(c, d)=1$，故可设$c=f^2$、

$d=l^2$，再由$x-y=2(c^2-d^2)=2pc_1{}^2$有$f^4-l^4=pc_1{}^2$，且$c_1<a_1=b_1c_1<a=2^ta_1<u=2ab$，此与$u$最小矛盾。

综i)、ii)、iii)所述，可知(d)无解。

习题 2　证明不定方程

$$x^4-2^yz^4=1$$

无正整数解。

证：当$y=1$时，$x^4-2^yz^4=1$变为$x^4-1^4=2(z^2)^2$，由习题1(c)知此种情形无解。当$y=2$时，由$x^4-4z^4=1$得$z=0$，此时也无正整数解。当$y\geqslant 3$时，设$z=u$是最小的正整数解，则$2\nmid u$，否则，如果$u=2u_1$，就有$x^4-2^{y+4}u_1{}^4=1$，即x、$y+4$、u_1也是解，但$u_1<u$，与u最小矛盾。显然x奇，从而，$(x^2+1,\ x^2-1)=2$。因此，$x^4-2^yu^4=1$给出

$$\begin{cases}x^2+1=2^{y-1}a^4\\x^2-1=2b^4\end{cases}\qquad(1)$$

或

$$\begin{cases}x^2+1=2b^4\\x^2-1=2^{y-1}a^4\end{cases}\qquad(2)$$

其中$u=ab$，$(a,b)=1$。如果（1）成立，则由$x^2-1=2b^4$得$0\equiv 2(\bmod 4)$，矛盾；如果（2）成立，就有$b^4-1=2^{y-2}a^4$，此即b、$y-2$、a也是方程$x^4-2^yz^4=1$的解，但$a<u=ab$，与u最小矛盾。

习题 3　证明不定方程组

$$x^2+y^2=z^2$$
$$y^2+z^2=t^2$$

无不全为0的整数解。

证：由$x^2+y^2=z^2$有$z^2-y^2=x^2$，把它和$z^2+y^2=t^2$相乘得

$$z^4-y^4=(xt)^2$$

由习题1(b)知，$z^4-y^4=(xt)^2$无不全为0的整数解，从而所给方程组也无全为0的整数解。

习题 4 利用上题证明：三边皆为有理整数的直角三角形之面积不可能是一完全平方数。

证： 设x、y、z是任一直角三角形的三条边，且均为正整数，z为斜边，则

$$x^2+y^2=z^2.$$

设 $(x、y)=d$，$x=dx_1$，$y=dy_1$，就有

$$d^2(x_1{}^2+y_1{}^2)=z^2$$

设$z=dz_1$得

$$x_1{}^2+y_1{}^2=z_1{}^2.$$

不妨设x_1为偶数，y_1为奇数．如果该直角三角形的面积为一平方数w^2，则有

$$\frac{xy}{2}=w^2$$

$$d^2\left(\frac{x_1}{2}\right)y_1=w^2$$

设$w=dw_1$，则有

$$x_1y_1=2w_1{}^2$$

因此 $x_1=2a^2$，$y_1=b^2$，$w_1=ab$，$(a,b)=1$

此时得到 $x_1{}^2+y_1{}^2=(2a^2)^2+(b^2)^2=b^4+4a^4=z_1{}^2$

由习题 1 $(a)x^4+4y^4=z^2$、$x>0$、$y>0$ 无解知道$b^4+4a^4=z_1{}^2$不能成立，故该直角三角形的面积$\frac{xy}{2}\neq w^2$。

习题 5 证明对任一正整数$n>2$，不定方程

$$y_n^n=y_{n-1}^{n-1}+y_{n-2}^{n-2}+\cdots+y_2^2$$

有无穷多组正整数解。

证： 对次数n使用归纳法。当$n=3$时

$$y_n^n=y_{n-1}^{n-1}+y_{n-2}^{n-2}+\cdots+y_2^2$$

变为$y_3^3=y_2^2$。对任意正整数a，取$y_3=a^2$、$y_2=a^3$就有$y_3^3=y_2^2$，故$n=3$时结论成立．归纳假定$n=k$时结论成立，即

$$y_k^k=y_{k-1}^{k-1}+y_{k-2}^{k-2}+\cdots+y_2^2$$

有无穷多组正整数解．当$n=k+1$时，欲证

$$y_{k+1}^{k+1}=y_k^k+y_{k-1}^{k-1}+\cdots+y_2^2$$

有无穷多组正整数解，由归纳假定知道只需要证明$y_{k+1}^{k+1}=2y_k^k$有正整数解就可以了．对于任意给定的正整数k，因为$(k,k+1)=1$，故总可找到正整数s、t，使

$$(k+1)s-kt=1$$

命　$y_{k+1}=2^s b^k$，$y_k=2^t b^{k+1}$

其中b为任一正整数．则

$$y_{k+1}^{k+1}=2^{s(k+1)}b^{k(k+1)}=2^{kt+1}b^{k(k+1)}=2(2^t)^k(b^{k+1})^k=2y_k^k$$

从而$n=k+1$时结论成立．故方程

$$y_n^n=y_{n-1}^{n-1}+y_{n-2}^{n-2}+\cdots+y_2^2$$

有无穷多组正整数解．

习题 6　求出不定方程

$$2x^n=z^{n-1}$$

的全部正整数解．

解：下面证明

$$x=2^{n-2}a^{n-1},\ \ z=2^{n-1}a^n$$

为方程$2x^n=z^{n-1}$的全部正整数解，其中a为任一正整数．

因为　$2(2^{n-2}a^{n-1})^n=2^{n(n-2)+1}a^{n(n-1)}$

$$=2^{(n-1)^2}a^{n(n-1)}=(2^{n-1}a^n)^{n-1}$$

所以　$$x=2^{n-2}a^{n-1},\ \ z=2^{n-1}a^n$$

为方程$2x^n=z^{n-1}$的解．另一方面，设x、z为不定方程$2x^n=z^{n-1}$的任一组正整数解，命

$$x=dx_1,\quad z=dz_1,\quad (x、z)=d$$

则$2x^n=z^{n-1}$变为

$$2dx_1{}^n=z_1{}^{n-1}$$

显然，$x_1{}^n|z_1{}^{n-1}$. 由 $(x_1, z_1)=1$ 有$x_1=1$，否则存在一个素数p合条件$p|x_1$、$p|z_1$，此与 $(x_1, z_1)=1$ 矛盾. 故

$$2dx_1{}^n=2d=z_1{}^{n-1}$$

$$z_1=(2d)^{\frac{1}{n-1}}$$

因此
$$d=2^{n-2}a^{n-1}$$

其中a为任意正整数. 故

$$x=dx_1=d=2^{n-2}a^{n-1}$$

$$z=dz_1=(2^{n-2}a^{n-1})2a=2^{n-1}a^n$$

所以，方程$2x^n=z^{n-1}$的全部正整数解由

$$x=2^{n-2}a^{n-1},\quad z=2^{n-1}a^n$$

给出. 其中a为任一正整数.

习题 7 设l、m、n为正整数，$(lm, n)=(ln, m)=(mn, l)=1$，则不定方程

$$x^l+y^m=z^n$$

有无穷多组正整数解.

证：因为 $(ln, m)=1$，所以存在正整数s、t，使得

$$sm-tln=1$$

对于任一正整数a，因为

$$\begin{aligned}&((a^n-1)^{tn})^l+((a^n-1)^s)^m\\&=(a^n-1)^{tnl}(1+(a^n-1)^{sm-tlm})\\&=(a^n-1)^{tnl}(1+(a^n-1))\\&=((a^n-1)^{tl}a)^n\end{aligned}$$

故对于任意正整数$a\neq 1$

$$x=(a^n-1)^{tn},\quad y=(a^n-1)^s,$$

$$z=(a^n-1)^{tl}a$$

为不定方程$x^l+y^m=z^n$的一组正整数解。由于a的任意性，从而该方程确有无穷多组正整数解。

又：条件 $(lm, n)=(ln,m)=(mn,l)=1$，可以减弱为$(ln, m)=1$。

习题 8 若$x^n+y^n=z^n$无整数解，则

$$x^{2n}+y^{2n}=z^2$$

也无整数解。

证：只需证明在题设条件下，不定方程

$$x^{2n}+y^{2n}=z^2$$

无正整数解就可以了。不妨设$(x,y)=1$，x偶，y奇，那么由$(x^n)^2+(y^n)^2=z^2$得出

$x^n=2ab$，$y^n=a^2-b^2$，$z=a^2+b^2$，$a>b>0$，$(a,b)=1$，$a+b\equiv 1 \pmod 2$

再不妨设$2|a$，$x^n=2ab$给出

$$\begin{cases}2a=c^n\\ b=d^n\end{cases} \qquad (1)$$

或

$$\begin{cases}a=d^n\\ 2b=c^n\end{cases} \qquad (2)$$

其中$x=cd$且$(c, d)=1$。由$(a,b)=1$、$2|a$知(2)不能成立。显然，$(a+b, a-b)=1$，从而，$y^n=a^2-b^2$给出

$$\begin{cases}a+b=e^n\\ a-b=f^n\end{cases} \qquad (3)$$

其中$y=ef$，$(e, f)=1$。由(1)、(3)分别得出

$$2a=c^n \quad 和 \quad 2a=e^n+f^n$$

从而有
$$e^n+f^n=c^n$$

此与$x^n+y^n=z^n$无解矛盾，故$x^n+y^n=z^n$无整数解，从而可推出$x^{2n}+y^{2n}=z^2$也无整数解。

§ 8 Марков方程

习题 1 推广上法以讨论不定方程

$$x_1^2+x_2^2+\cdots+x_n^2=nx_1\cdots x_n.$$

解：本题中所指"上法"，是指关于不定方程

$$x^2+y^2+z^2=3xyz \tag{1}$$

求解方法的两个定理，即

定理 1 若x_0、y_0、z_0是(1)的解，则x_0、y_0、$3x_0y_0-z_0$也是(1)的解。

定理 2 凡(1)的解，可用定理1中方法，由$x=y=z=1$一解得出。

为解不定方程

$$x_1^2+x_2^2+\cdots+x_n^2=nx_1\cdots x_n \tag{1'}$$

我们把定理1和定理2作如下推广：

定理1′ 若x_1，$x_2,\cdots,x_n$是(1′)的解，则x_1，$x_2,\cdots,x_{n-1}$，$nx_1\cdots x_{n-1}-x_n$也是(1′)的解。

因为

$$\begin{aligned}
&x_1^2+x_2^2+\cdots+x_{n-1}^2+(nx_1\cdots x_{n-1}-x_n)^2\\
&=x_1^2+x_2^2+\cdots+x_{n-1}^2+n^2x_1^2\cdots x_{n-1}^2-2nx_1\cdots x_n+x_n^2\\
&=x_1^2+x_2^2+\cdots+x_n^2+n^2x_1^2\cdots x_{n-1}^2-2nx_1\cdots x_n\\
&=nx_1\cdots x_n+n^2x_1^2\cdots x_{n-1}^2-2nx_1\cdots x_n\\
&=n^2x_1^2\cdots x_{n-1}^2-nx_1\cdots x_n\\
&=nx_1\cdots x_{n-1}(nx_1\cdots x_{n-1}-x_n)
\end{aligned}$$

故定理1′成立。

定理2′ 凡(1′)的解，可用定理1′中方法，由$x_1=x_2=\cdots=x_n=1$一解得出。

为了证明定理(2′)，先证下面一个引理。

引理　当$n>3$时，不等式

$$(n-1)+w^2\leqslant nw$$

成立，其中$1\leqslant w\leqslant n-1$。

i）当$w=1$，$n-1$时等号成立。

ii）当$1<w<\frac{n}{2}$时，设

$$f(w)=w^2-nw+(n-1)$$

则　$f'(w)=2w-n$

显然$f'(w)<0$，$f(w)$单调减少．又因为

$$f(2)=2^2-2n+(n-1)=3-n<0$$

所以，当$1<w<\frac{n}{2}$时，结论成立。

iii）当$\frac{n}{2}\leqslant w<n-1$时，$f'(w)\geqslant 0$、$f(w)$单调增加，又因为

$$f(n-2)=(n-2)^2-n(n-2)+(n-1)=3-n<0$$

所以，当$\frac{n}{2}\leqslant w<n-1$时，结论成立。

由i）～iii）知引理成立。

下面证明定理2′。

1）若$x_1=x_2=\cdots=x_n$，则显然有

$$x_1=x_2=\cdots=x_n=1$$

2）若$x_1=x_2=\cdots=x_{n-1}=x\neq x_n$，则

$$(n-1)x^2+x_n^2=nx^{n-1}x_n$$

从而，$x^2|x_n^2$，$x|x_n$。设$x_n=wx$，$w>0$，则$(n-1)+w^2=nwx^{n-2}$，所以$w|(n-1)$．显然$w\neq 1$，否则$x_n=x$，此与$x_1=x_2=\cdots=x_{n-1}=x\neq x_n$相矛盾，故有$1<w\leqslant n-1$．由引理可知，当$1<w<n-1$时，$(n-1)+w^2=nwx^{n-2}$无整数解，因此$w=n-1$．此时

$$(n-1)+(n-1)^2=n(n-1)x^{n-2}$$

$$n = nx^{n-2}$$

$$x = 1$$

$$x_n = wx = n-1$$

故有 $x_1 = x_2 = \cdots = x_{n-1} = 1$，$x_n = n-1$

注意到 $x_n = n\cdot\underbrace{1\cdot 1\cdots\cdots 1}_{(n-1)\text{个}} - 1$，可知此解可由

$$\underbrace{(1,\ 1,\ \cdots\cdots,\ 1)}_{n\text{个}}$$

经定理1′得出

3）今可假定 $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_{n-1} \leqslant x_n$，如能由此证明 $nx_1\cdots x_{n-1} - x_n < x_n$，则就可使 $x_1 + \cdots + x_n$ 的值逐步变小，经有限步后，必可使 x_1，$x_2\cdots$，x_n 中有 $n-1$ 个，或者 n 个相等，从而可归入 1）2）。由

$$x_n^2 - nx_1\cdots x_n + x_1^2 + \cdots + x_{n-1}^2 = 0$$

有 $2x_n = nx_1\cdots x_{n-1} \pm \sqrt{n^2x_1^2\cdots x_{n-1}^2 - 4(x_1^2 + \cdots + x_{n-1}^2)}$

而当 $n > 3$，$x_1 \leqslant x_2 \leqslant \cdots \leqslant x_{n-1}$ 且 $x_1, \cdots, x_{n-1}$ 不全为 1（全为 1 的情形归入2)）时，显然有

$$(n-1)x_1^2\cdots x_{n-1}^2 > x_1^2 + \cdots + x_{n-1}^2$$

即 $n^2x_1^2\cdots x_{n-1}^2 - 4(x_1^2 + \cdots x_{n-1}^2) > (n-2)^2x_1^2\cdots x_{n-1}^2$.

如果 $2x_n = nx_1\cdots x_{n-1} - \sqrt{n^2x_1^2\cdots x_{n-1}^2 - 4(x_1^2 + \cdots + x_{n-1}^2)}$

就有 $2x_n < nx_1\cdots x_{n-1} - (n-2)x_1\cdots x_{n-1} = 2x_1\cdots x_{n-1}$

即 $$x_n < x_1\cdots x_{n-1}$$

但是 $$nx_n^2 \geqslant x_1^2 + \cdots + x_n^2 = nx_1\cdots x_n$$

即 $$x_n \geqslant x_1\cdots x_{n-1}$$

此与 $x_n < x_1\cdots x_{n-1}$ 矛盾，故一定有

$$2x_n = nx_1\cdots x_{n-1} + \sqrt{n^2x_1^2\cdots x_{n-1}^2 - 4(x_1^2 + \cdots + x_{n-1}^2)}$$

所以 $$2x_n > nx_1\cdots x_{n-1}$$

即 $$nx_1\cdots x_{n-1} - x_n < x_n.$$

习题 2　求出

$$x_1^2+x_2^2+x_3^2+x_4^2=4x_1x_2x_3x_4,$$
$$x_1\leqslant x_2\leqslant x_3\leqslant x_4\leqslant 100$$

之诸解。

解：由习题1知道，此方程的所有解可由解（1，1，1，1）经定理1′逐步求出，现列表如下：

x_4	1	3	11	41
x_3	1	1	3	11
x_2	1	1	1	1
x_1	1	1	1	1

习题 3　求证

$$2x^4-y^4=z^4$$

有无穷多解。

证：对任意整数a，取$x=y=a$、$z=a^2$，就有

$$2a^4-a^4=(a^2)^2$$

此即（a,a,a^2）为方程$2x^4-y^4=z^2$的一组整数解。由于a的任意性，故方程

$$2x^4-y^4=z^2$$

有无穷多解。

§ 9　解方程$x^3+y^3+z^3+w^3=0$

习题 1　$\alpha^3+\beta^3+\gamma^3+\delta^3=0$之有理解可由

$$\alpha=\sigma(-(\xi-3\eta)(\xi^2+3\eta^2)+1)$$
$$\beta=\sigma((\xi+3\eta)(\xi^2+3\eta^2)-1)$$
$$\gamma=\sigma((\xi^2+3\eta^2)^2-(\xi+3\eta))$$

$$\delta=\sigma((\xi^2+3\eta^2)^2-(\xi-3\eta))$$

表之，此处ξ、η为有理数。

若$\sigma=1$，ξ及η为整数，可得出$x^3+y^3+z^3+w^3=0$之无穷个整数解，但这并不包括所有的整数解。

试证

$$\alpha=1,\ \beta=12,\ \gamma=-10,\ \delta=-9$$

即其一例。

证：因为$1^3+12^3+(-10)^3+(-9)^3=0$

即 $\alpha=1,\ \beta=12,\ \gamma=-10,\ \delta=-9$

为方程$x^3+y^3+z^3+w^3=0$的一组整数解。下面证明此组解不能由所给的公式给出。因若不然，就有

$$\begin{cases}(3\eta-\xi)(\xi^2+3\eta^2)+1=1 & (1)\\ (3\eta+\xi)(\xi^2+3\eta^2)-1=12 & (2)\\ (\xi^2+3\eta^2)^2-(\xi+3\eta)=-10 & (3)\\ (\xi^2+3\eta^2)^2-(\xi-3\eta)=-9 & (4)\end{cases}$$

由(1)有$\xi=3\eta$或$\xi=\eta=0$，代入(4)就有

$$144\eta^4=-9$$

或

$$0=-9$$

这都不可能。故$\sigma=1$时，取ξ、η为整数，所给公式能得出方程

$$x^3+y^3+z^3+w^3=0$$

的无穷多组整数解（此点可直接验证），但并不能包含所有整数解。

习题2 证恒等式

$$y^{12}=(9x^4)^3+(3xy^3-9x^4)^3+(y^4-9x^3y)^3.$$

因之得

$$5^{12}=9^3+366^3+580^3=144^3+606^3+265^3.$$

证：$(9x^4)^3+(3xy^3-9x^4)^3+(y^4-9x^3y)^3$

$$=729x^{12}+27x^3y^9-3(3xy^3)^2 9x^4$$

$$+3(3xy^3)(9x^4)^2-729x^{12}+y^{12}$$
$$-3(y^4)^2 9x^3y+3y^4(9x^3y)^2-729x^9y^3=y^{12}$$

在恒等式

$y^{12}=(9x^4)^3+(3xy^3-9x^4)^3+(y^4-9x^3y)^3$中，取$x=1$、$y=5$得

$$5^{12}=9^3+366^3+580^3$$

取$x=2$、$y=5$得

$$5^{12}=144^3+606^3+265^3.$$

习题 3　由上习题，证明有n存在，使

$$n=x^3+y^3+z^3,$$

$x\geqslant 0$，$y\geqslant 0$，$z\geqslant 0$之解数$>\frac{1}{3}n^{\frac{1}{12}}$.

证：当$n=5^{12}$时，

$$(9,\ 366,\ 580),\quad (144,\ 606,\ 265)$$

是方程$n=x^3+y^3+z^3$合条件$x\geqslant 0$，$y\geqslant 0$，$z\geqslant 0$ 的二组整解。所以，方程

$$5^{12}=x^3+y^3+z^3$$

的非负解数$\geqslant 2>\frac{5}{3}=\frac{1}{3}\ (5^{12})^{\frac{1}{12}}$.

习题 4　证明

$$(3a^2+5ab-5b^2)^3+(4a^2-4ab+6b^2)^3+(5a^2-5ab-3b^2)^3$$
$$=(6a^2-4ab+4b^2)^3.$$

证：因为

$$(3a^2+5ab-5b^2)^3+(5a^2-5ab-3b^2)^3$$
$$=(8a^2-8b^2)\left[(3a^2+5ab-5b^2)^2\right.$$
$$-(3a^2+5ab-5b^2)(5a^2-5ab-3b^2)$$
$$\left.+(5a^2-5ab-3b^2)^2\right]$$

$$=(8a^2-8b^2)[9a^4+25a^2b^2+25b^4+30a^3b-30a^2b^2$$
$$-50ab^3-15a^4+15a^3b+9a^2b^2-25a^3b+25a^2b^2+15ab^3$$
$$+25a^2b^2-25ab^3-15b^4+25a^4+25a^2b^2+9b^4-50a^3b$$
$$-30a^2b^2+30ab^3]$$
$$=8(a^2-b^2)(19a^4-30a^3b+49a^2b^2-30ab^3+19b^4).$$

$$(6a^2-4ab+4b^2)^3-(4a^2-4ab+6b^2)^3$$
$$=8(3a^2-2ab+2b^2)^3-8(2a^2-2ab+3b^2)^3$$
$$=8\{(a^2-b^2)[(3a^2-2ab+2b^2)^2+(3a^2-2ab+2b^2)$$
$$(2a^2-2ab+3b^2)+(2a^2-2ab+3b^2)^2]\}$$
$$=8\{(a^2-b^2)[9a^4+4a^2b^2+4b^4-12a^3b+12a^2b^2-8ab^3$$
$$+6a^4-6a^3b+9a^2b^2-4a^3b+4a^2b^2-6ab^3+4a^2b^2-4ab^3$$
$$+6b^4+4a^4+4a^2b^2+9b^4-8a^3b$$
$$+12a^2b^2-12ab^3]\}$$
$$=8(a^2-b^2)(19a^4-30a^3b+49a^2b^2-30ab^3+19b^4)$$

所以 $(3a^2+5ab-5b^2)^3+(4a^2-4ab+6b^2)^3+$

$$+(5a^2-5ab-3b^2)^3=(6a^2-4ab+4b^2)^3.$$

本章末习题

习题1 求出下列不定方程的全部正整数解：

1）$2^x-3^y=1$,

2）$3^x-2^y=1$,

解：1）$2^x-3^y=1$只有一组正整数解，即$x=2$，$y=1$. 对 $2^x-3^y=1$取模3得

$$2^x\equiv(3-1)^x\equiv(-1)^x\equiv 1 \pmod 3,$$

所以x为偶数. 设为$x=2X$，原方程变为

$$(2^X+1)(2^X-1)=3^y$$

$(2^X+1,\ 2^X-1)=1$，故$2^X-1=1$，$X=1$，$x=2$，$y=1$.

2）$3^x-2^y=1$只有两组正整数解，即$x=y=1$；$x=2$，$y=3$. $x=y=1$显然是该方程的解．当$x>1$、$y>1$时，对该方程取模4得

$$3^x\equiv(4-1)^x\equiv(-1)^x\equiv1\ (\mathrm{mod}4)$$

所以x为偶数．设$x=2X$，原方程变为

$$(3^X+1)(3^X-1)=2^y$$

$(3^X+1,\ 3^X-1)=2$，故

$3^X-1=2$，$3X+1=2^{y-1}$，$X=1$，$y=3$，即$x=2$，$y=3$.

习题2　证明不定方程

$$5^x=2^y+3^z$$

只有三组整数解：$x=y=z=1$；$x=1$、$y=2$、$z=0$；$x=2$、$y=4$、$z=2$.

证：（一）当y为奇数，$y=2Y+1$时

i）当$Y=0$时，$5^x=2^{2Y+1}+3^z$变成

$$5^x=2+3^z$$

显然有解$x=y=z=1$．现证该方程无整数解$x>1$、$z>1$．对$5^x=2+3$取模5得

$$0\equiv2+3^z(\mathrm{mod}5)$$

从而$z\equiv1\ (\mathrm{mod}4)$．把$5^x=2+3^z$写成

$$(4+1)^x-(4-1)^z=2$$

即$$\left(4^x+\binom{x}{1}4^{x-1}+\cdots+\binom{x}{x-2}4^2+\binom{x}{x-1}4+1\right)-$$

$$-\left(4^z-\binom{z}{1}4^{z-1}+\cdots-\binom{z}{z-2}4^2+\binom{z}{z-1}4-1\right)=2$$

从而有　$$\binom{x}{x-1}4\equiv\binom{z}{z-1}4(\mathrm{mod}16)$$

即　$$x\equiv z(\mathrm{mod}4)$$

再由$z\equiv1\ (\mathrm{mod}4)$得$x\equiv z\equiv1\ (\mathrm{mod}4)$．把方程$5^x=2+3^z$取模7得

$$4^z-2^x\equiv2\ (\mathrm{mod}7)$$

结合$x\equiv z\equiv 1\pmod 4$ 立得

$$x\equiv z\equiv 1\pmod{12}.$$

把方程$5^x=2+3^z$同解地写成

$$5^x-5=3^z-3$$

即
$$5(5^{x-1}-1)=3(3^{z-1}-1) \qquad (1)$$

设$x-1=2^t a$，$2\nmid a$。由$x\equiv 1\pmod{12}$知，$t\geqslant 2$且$3\mid a$，从而(1)可写成

$$5\left(5^{\frac{x-1}{2}}+1\right)\left(5^{\frac{x-1}{2^2}}+1\right)\left(5^{\frac{x-1}{2^3}}+1\right)\cdots\left(5^{\frac{x-1}{2^{t-1}}}++1\right)$$

$$\cdot(5^a+1)(5^a-1)=3(3^{z-1}-1) \qquad (1')$$

又因为 $5^a+1=(5+1)(5^{a-1}-5^{a-2}+\cdots+5^2-5+1)$

且 $5^{a-1}-5^{a-2}+\cdots+5^2-5+1$

$\equiv(6-1)^{a-1}-(6-1)^{a-2}+\cdots+(6-1)^2-(6-1)+1$

$\equiv(-1)^{a-1}-(-1)^{a-2}+\cdots+(-1)^2-(-1)+1$

$\equiv 1+1+\cdots+1\equiv a\equiv 0\pmod 3$

故有$9\mid 5^a+1$，结合(1′)得$3\mid 3^{z-1}-1$。但是，$z>1$，故此不可能。因此，方程

$$5^x=2+3^z$$

的确无整数解$x>1$，$z>1$。

ii) 当$Y\geqslant 1$时，因为 $(-1)^z\equiv 1\pmod 4$，故z为偶数。设$z=2z_1$，从而$5^x=2^{2Y+1}+3^z$变成$5^x-9^{z_1}=2\cdot 4^Y$。但是5^x的个位数字是5，9^{z_1}的个位数字是9或1，$2\cdot 4^Y$的个位数字是8或2，因此$5^x-9^{z_1}=2\cdot 4^Y$不能成立。

由i)、ii)可知，方程$5^x=2^y+3^z$在y为奇数时，只有唯一解$x=y=z=1$。

(二) 当y为偶数，$y=2Y$时

i) 当$Y=0$时，原方程变为$5^x=1+3^z$，此种情形显然无解，否则$1\equiv 0\pmod 2$。

ii) 当$Y=1$时，原方程变为$5^x=4+3^z$，给出$x=1$、$z=0$，从而$x=1$、$y=2$、$z=0$为一组解。此种情形若原方程有解$z>0$，那么由

$(-1)^X\equiv 1\ (\bmod 3)$可设$x=2x_1$。如果$x_1=0$就有$1=4+3^z$，此不可能。因此有$x_1\geqslant 1$，从而$5^X=4+3^z$给出

$$(5^{X_1}+2)(5^{X_1}-2)=3^z$$

另外，由于$(5^{X_1}+2,\ 5^{X_1}-2)=1$，所以有

$$5^{X_1}-2=1$$

此不可能。故当$Y=1$时，原方程只有唯一解

$$x=1、y=2、z=0。$$

iii) 当$Y\geqslant 2$时，$5^X=4^Y+3^z$给出

$$(-1)^z\equiv 1\ (\bmod 4)$$

$$1\equiv(-1)^X(\bmod 3)$$

故可设$x=2x_1$，$z=2z_1$，从而

$$(5^{X_1}+3^{z_1})(5^{X_1}-3^{z_1})=4^Y$$

如果z_1是偶数，$5^{X_1}+3^{z_1}\equiv 2\ (\bmod 4)$，$(5^{X_1}+3^{z_1})\cdot(5^{X_1}-3^{z_1})=4^Y$给出

$$5^{X_1}+3^{z_1}=2$$

$$5^{X_1}-3^{z_1}=2^{2Y-1}$$

此不可能。

如果z_1是奇数，$5^{X_1}-3^{z_1}\equiv 2\ (\bmod 4)$，$(5^{X_1}+3^{z_1})(5^{X_1}-3^{z_1})=4^Y$就给出

$$5^{X_1}-3^{z_1}=2$$

$$5^{X_1}+3^{z_1}=2^{2Y-1}$$

如果$z_1=1$或$x_1=1$，由$5^{X_1}-3^{z_1}=2$都会得出$z_1=x_1=1$。再由$5^{X_1}+3^{z_1}=2^{2Y-1}$得$Y=2$。故此时原方程有解

$$x=2,\ y=4,\ z=2$$

再由（一）i）可知，方程

$$5^{X_1}-3^{z_1}=2$$

无整数解$x_1>1$、$z_1>1$。故当$Y\geqslant 2$时，原方程有唯一解$x=z=2$，$y=4$。

综上所述，不定方程

$$5^x=2^y+3^z$$

只有三组整数解：$x=y=z=1$；$x=1$，$y=2$，$z=0$；$x=2$，$y=4$，$z=2$。

习题3 求出不定方程

$$x^y = y^x$$

的全部有理数解.

解：我们将证明$x=y\neq 0$是方程$x^y=y^x$的全部有理数解. 显然$x=y\neq 0$是$x^y=y^x$的解.另一方面，设x、y是方程$x^y=y^x$的任一组有理数解，$xy\neq 0$.不失一般，可设

$$x=\frac{n}{m},\quad y=\frac{s}{r},\quad (m,\ n)=(r,\ s)=1$$

由

$$\left(\frac{n}{m}\right)^{\frac{s}{r}}=\left(\frac{s}{r}\right)^{\frac{n}{m}}$$

$$\left[\left(\frac{n}{m}\right)^{\frac{s}{r}}\right]^{mr}=\left[\left(\frac{s}{r}\right)^{\frac{n}{m}}\right]^{mr}$$

$$\left(\frac{n}{m}\right)^{ms}=\left(\frac{s}{r}\right)^{nr}$$

$$m^{ms}s^{nr}=n^{ms}r^{nr}$$

有

$$\begin{cases} m^{ms}=r^{nr} \\ n^{ms}=s^{nr} \end{cases} \tag{1}$$

设

$$\begin{aligned} & m=d_1m_1,\ r=d_1r_1,\ m_1>0,\ r_1>0, \\ & \quad (m,\ r)=|d_1|; \\ & n=d_2n_2,\ s=d_2s_2,\ n_2>0,\ s_2>0, \\ & \quad (n,\ s)=|d_2|. \end{aligned} \tag{2}$$

把（2）代入（1），$m^{ms}=r^{nr}$变成

$$\begin{aligned} & (d_1m_1)^{d_1m_1d_2s_2}=(d_1r_1)^{d_2n_2d_1r_1} \\ & |d_1|^{m_1s_2}m_1^{m_1s_2}=|d_1|^{n_2r_1}r_1^{n_2r_1} \\ & |d_1|^{m_1s_2-n_2r_1}m_1^{m_1s_2}=r_1^{n_2r_1} \end{aligned} \tag{3}$$

$n^{ms}=s^{nr}$变成

$$\begin{aligned} & (d_2n_2)^{d_1m_1d_2s_2}=(d_2s_2)^{d_2n_2d_1r_1} \\ & |d_2|^{m_1s_2}n_2^{m_1s_2}=|d_2|^{n_2r_1}s_2^{n_2r_1} \\ & |d_2|^{m_1s_2-n_2r_1}n_2^{m_1s_2}=s_2^{n_2r_1} \end{aligned} \tag{4}$$

i)　当$m_1s_2=n_2r_1$时，（3）、（4）给出

$$m_1=r_1=1,\ n_2=s_2=1$$

再由（2）得　$m=r=d_1$，$n=s=d_2$

故　$$x=\frac{n}{m}=\frac{d_2}{d_1},\quad y=\frac{s}{r}=\frac{d_2}{d_1}$$

此即　$x=y$

ii）当$m_1s_2>n_2r_1$时，（3）、（4）给出$m_1=n_2=1$．此时$r=r_1m$，$s=s_2n$。

由　$$\left(\frac{n}{m}\right)^{\frac{s}{r}}=\left(\frac{s}{r}\right)^{\frac{n}{m}}$$

有　$$\left(\frac{n}{m}\right)^{\frac{s_2-r_1}{r_1}}=\pm\left(\frac{s_2}{r_1}\right)$$

从而有
$$\begin{cases} n^{\frac{s_2-r_1}{r_1}}=\pm s_2 & (5)\\ m^{\frac{s_2-r_1}{r_1}}=\pm r_1 & (6)\end{cases}$$

设$(n,\ s_2)=D$，$n=n'D$，$s_2=s_2'D$．显然$D>1$．由（5）有

$$(n'D)^{\frac{s_2-r_1}{r_1}}=\pm s_2'D$$

$$D^{\frac{s_2-r_1}{r_1}}=D$$

$$\frac{s_2-r_1}{r_1}=1$$

$$s_2=2r_1$$

但$(s_2,\ r_1)=1$，故$s_2=2$，$r_1=1$，$r=m$，$s=2n$，此种情形

$$\left(\frac{n}{m}\right)^{\frac{s}{r}}=\left(\frac{s}{r}\right)^{\frac{n}{m}}$$

给出$n^2=\pm2n$，$n=0$，$x=0$，这不可能．故当$m_1s_2>n_2r_1$时，原方程

无解.

iii) 当$m_1s_2<n_2r_1$时，用ii)中相同的方法可证原方程无解.

由i)～iii)可知，方程$x^y=y^x$的全部有理数解由$x=y=a$给出，其中a为非零有理数.

习题4 证明不定方程

$$x^y=y^x+1$$

只有二组正整数解：$x=2$、$y=1$；$x=3$、$y=2$.

证：（一）如果x、y同奇、同偶，则都有

$$0\equiv 1\pmod 2$$

此种情形无解.

（二）如果x偶y奇．$y=1$时，$x^y=y^x+1$给出$x=2$．$y\geqslant 3$时无解，否则，$x^y=y^x+1$给出$0\equiv 2\pmod 4$，矛盾.

（三）如果x奇y偶且$x>1$，下面证明

$$x^y=y^x+1$$

只有一组正整数解$x=3$，$y=2$.

设$y=2^ta$，$2\nmid a$，$t\geqslant 1$．当$t=1$时，原方程可写成

$$(x^a+1)(x^a-1)=2^xa^x \tag{1}$$

由于$(x^a+1，x^a-1)=2$；因此（1）给出

$$2^{x-1}|x^a+1$$

或

$$2^{x-1}|x^a-1$$

又因 $x^a+1=(x+1)(x^{a-1}-x^{a-2}+\cdots-x+1)$

$x^a-1=(x-1)(x^{a-1}+x^{a-2}+\cdots+x+1)$

且 $2\nmid(x^{a-1}-x^{a-2}+\cdots-x+1)$

$2\nmid(x^{a-1}+x^{a-2}+\cdots+x+1)$

故有 $2^{x-1}|x+1$

或 $2^{x-1}|x-1$.

当$x>1$时，$2^{x-1}|x-1$显然不可能成立，由$2^{x-1}|x+1$给出$x=3$，由

$3^2=2^3+1$ 知道 $x=3$、$y=2$ 为一组解．如果 $y\geqslant 4$，由归纳法易证 $3^y>$ $>y^3+1$，因而 $3^y=y^3+1$ 无解．所以，$t=1$ 时原方程只有一组解 $x=3$、$y=2$．下面再证明 $t\geqslant 2$ 时，原方程无解．当 $t\geqslant 2$ 时，原方程可写成

$$\left(x^{\frac{y}{2}}+1\right)\left(x^{\frac{y}{2^2}}+1\right)\cdots\cdots\left(x^{\frac{y}{2^{t-1}}}+1\right)\left(x^{a}+1\right)$$

$$\cdot\left(x^{a}-1\right)=2^{tx}a^{x} \qquad (2)$$

由于 x 为奇数，且 $1\leqslant k\leqslant t-1$ 时 $\frac{y}{2^k}$ 为偶数，因此

$$x^{\frac{y}{2^k}}+1\equiv 2\,(\mathrm{mod}\,4)\,;\qquad 2\,\|\,x^{\frac{y}{2^k}}+1,\quad 1\leqslant k\leqslant t-1$$

注意到 $(x^a+1, x^a-1)=2$，因此（2）给出

$$2^{tx-t}\mid x^a+1$$

或 $$2^{tx-t}\mid x^a-1,$$

由前证即知 $$2^{tx-t}\mid x+1$$

或 $$2^{tx-t}\mid x-1$$

但当 $x\geqslant 3$，$t\geqslant 2$ 时，

$$2^{tx-t}=(2^t)^{x-1}\geqslant 4^{x-1}>x\pm 1$$

故 $$2^{tx-t}\nmid x\pm 1$$

也就是说，$t\geqslant 2$、$x>1$ 时，原方程无正整数解．

显然，$x=1$ 时，$y=0$．

综上所述，不定方程 $x^y=y^x+1$ 只有两组正整数解 $x=2$，$y=1$；$x=3$，$y=2$．

习题5　求出不定方程

$$(x+y)^y=x^{y+1}+1$$

的全部正整数解．

解：下面证明此方程只有两组正整数解

$$x=y=1;\ x=y=2.$$

（一）如果 x 奇、y 奇

i）$x=1$ 时 $2^y=1^{y+1}+1$ 给出 $x=y=1$．

ii）$x>1$ 时，$(x+1)^y=x^{y+1}+1$ 给出 $0\equiv 2\,(\mathrm{mod}\,4)$．因此 x 奇、y 奇

时，方程只有一组解$x=y=1$。

（二）如果x奇、y偶

先把不定方程

$$(x+1)^y=x^{y+1}+1$$

作如下变形：

$$(x+1)^y-1=x^{y+1}$$

$$(x+1)^{y-1}+(x+1)^{y-2}+\cdots+(x+1)+1=x^y$$

$$(x+1)[(x+1)^{y-2}+(x+1)^{y-3}+\cdots+(x+1)+1]$$
$$=(x-1)(x^{y-1}+x^{y-2}+\cdots+x+1) \qquad (1)$$

注意到y为偶数时

$$\frac{x^{y-1}+x^{y-2}+\cdots+x+1}{x+1}=x^{y-2}+x^{y-4}+\cdots+x^2+1$$

可以得到

$$(x+1)^{y-2}+(x+1)^{y-3}+\cdots+(x+1)+1$$
$$=(x-1)(x^{y-2}+x^{y-4}+\cdots+x^2+1) \qquad (2)$$

但（2）给出$1\equiv 0 \pmod 2$，故x奇、y偶时方程无解。

（三） 如果x偶、y奇

（1）给出$0\equiv 1 \pmod 2$，此时原方程也无解。

（四） 如果x偶，y偶

i) $x=2$时，$(x+1)^y=x^{y+1}+1$给出$3^y=2^{y+1}+1$。设$y=2y_1$

可得

$$(3^{y_1}+1)(3^{y_1}-1)=2^{2y_1+1}$$

由 $(3^{y_1}+1,\ 3^{y_1}-1)=2$ 得

$$3^{y_1}-1=2,\ y_1=1,\ y=2y_1=2$$

故$x=2$，$y=2$是原方程的一组解，也就是说，$x=2$时原方程只有一组正整数解$x=y=2$。

ii) $x>2$，$y>2$时，由$(x+1)^y=x^{y+1}+1$有

$$x^y + C_y^1 x^{y-1} + \cdots + C_y^2 x^2 + C_y^1 x = x^{y+1}$$

因此$x \mid C_y^1$，即$x \mid y$.设$y=mx$, $x=2^t x_1$, $t\geqslant 1$，$2\nmid x_1$；$y=2^t m x_1$.把$y=2^t m x_1$代入下式

$$(x+1)^y = x^{y+1}+1$$

得
$$(2^t x_1+1)^{2^t m x_1} = (2^t x_1)^{2^t m x_1+1}+1$$

$$\left((2^t x_1+1)^{2^{t-1} m x_1}\right)^2 - 1 = 2^{2^t t m x_1 + t} \cdot x_1^{2^t m x_1+1}$$

又因为 $\left((2^t x_1+1)^{2^{t-1}mx_1}+1,\ (2^t x_1+1)^{2^{t-1}mx_1}-1\right)=2$

所以
$$\begin{cases}(2^t x_1+1)^{2^{t-1}mx_1}+1 = 2^{2^t t m x_1+t-1} a^{2^t m x_1+1} \\ (2^t x_1+1)^{2^{t-1}mx_1}-1 = 2b^{2^t m x_1+1}\end{cases} \qquad (3)$$

或
$$\begin{cases}(2^t x_1+1)^{2^{t-1}mx_1}+1 = 2b^{2^t m x_1+1} \\ (2^t x_1+1)^{2^{t-1}mx_1}-1 = 2^{2^t t m x_1+t-1} a^{2^t m x_1+1}\end{cases} \qquad (4)$$

其中$x_1=ab$，$(a, b)=1$．如果（3）成立，由

$$(2^t x_1+1)^{2^{t-1}mx_1}-1 = 2b^{2^t m x_1+1}$$

有$2^t x_1 \mid 2b^{2^t m x_1+1}$．显然$t=1$，否则$2\mid b$，$2\mid x_1$，此与$2\nmid x_1$相矛盾．而$t=1$时$x_1 \mid b^{2mx_1+1}$，由$x_1=ab$, $(a, b)=1$有$x_1=b$，$a=1$，从而（3）给出

$$2^{2mx_1-1} - x_1^{2mx_1+1} = 1$$

但$x=2x_1>2$，$x_1>1$，故此不可能．如果（4）成立，

$$(2^t x_1+1)^{2^{t-1}mx_1}-1 = 2^{2^t t m x_1+t-1} a^{2^t m x_1+1}$$

给出
$$2^t x_1 \mid 2^{2^t tmx_1+t-1} a^{2^t m x_1+1}$$

$$x_1 \mid a^{2^t m x_1+1}$$

因此，$x_1=a$，$b=1$．此时（4）中的

$$(2^t x_1+1)^{2^{t-1}mx_1}+1=2b^{2^t mx_1}+1$$

变为 $$(2^t x_1+1)^{2^{t-1}mx_1}=1$$

此也不可能.

习题6 证明$x=7$，$y=20$是不定方程

$$1+x+x^2+x^3+y^2$$

唯一使x为素数的解.

证：下面证明该方程只有解$x=-1$、$y=0$；$x=0$、$y=\pm1$；$x=1$、$y=\pm2$；$x=7$、$y=\pm20$.从而本题断语真实.

方程可以变形为 $y^2=(x+1)(x^2+1)$

显然$x\geqslant-1$，否则$y^2<0$；而$x=-1$、0、1时，由原方程可解出$y=0$、±1、±2.

（一）如果x为非零偶数，易证$(x+1,\ x^2+1)=1$，$y^2=(x+1)\cdot(x^2+1)$ 给出

$x+1=a^2$，$x^2+1=b^2$，$y=ab$，$(a,\ b)=1$. 但$x^2+1\neq b^2$，故此时方程无解.

（二）如果x为大于1的奇数，下面给出方程只有解$x=7$，$y=\pm20$的证明. 此种条件下，易证$(x+1,\ x^2+1)=2$，由$y^2=(x+1)(x^2++1)$有

$$x+1=2m^2,\ x^2+1=2n^2,\ y=2mn,\ (m,\ n)=1,\ 2\nmid n.$$

由 $$n^2=\frac{x^2+1}{2}=\frac{(2m^2-1)^2+1}{2}=\frac{4(m^2)^2-4m^2+2}{2}$$

$$=2(m^2)^2-2m^2+1=(m^2-1)^2+(m^2)^2$$

有 $$(m^2-1)^2+(m^2)^2=n^2 \tag{1}$$

i）当m为奇数时，（1）给出

$m^2=u^2-v^2$，$m^2-1=2uv$，$n=u^2+v^2$，$(u,\ v)=1$，$u>v>0$，u，v一奇一偶，$(u+v,\ u-v)=1$. 因此

$$m^2=u^2-v^2=(u+v)(u-v)$$

给出 $$u-v=a^2,\ u+v=b^2$$

由　　$m^2=u^2-v^2$，$m^2-1=2uv$

有　　$u^2-v^2-2uv=(u-v)^2-2v^2=1$

从而就有　　$a^4-2v^2=1$

即　　$a^4+v^4=(v^2+1)^2$

但此不可能．因此m为奇数时，（1）不可解，从而原方程无解．

　　ii）　当m为偶数时，（1）给出

$$m^2-1=u^2-v^2,\quad m^2=2uv,\quad n=u^2+v^2.$$

由$m^2=2uv$有

$$\begin{cases}u=2a^2\\ v=b^2\end{cases}$$

或

$$\begin{cases}u=b^2\\ v=2a^2\end{cases}$$

其中$m=2ab$，$(a,\ b)=1$．不妨设前一式成立．由

$$m^2-1=u^2-v^2,\quad m^2=2uv$$

有　$2uv-(u^2-v^2)=(u+v)^2-2u^2=1$

$$2u^2=(u+v+1)(u+v-1)$$

因为u、v一奇一偶，故可设$u+v=2s+1$．

又因$u=2a^2$，从而有

$$8a^4=(2s+2)2s$$

即　　$2a^4=(s+1)s$

但是$(s+1,\ s)=1$，故有

$$s=t^4,\quad s+1=2r^4$$

或　　$s=2r^4$，$s+1=t^4$

其中　$a=tr$，$(t,\ r)=1$．

所以　　$t^4-2r^4=-1$

或　　$t^4-2r^4=1$

即　　$(r^2)^4-t^4=(r^4-1)^2$

或　　$t^4+(r^2)^4=(r^4+1)^2$

由本章7节习题1（b）、$(r^2)^4-t^4=(r^4-1)^2$的解为$r^2=0$或$r^4-1=$
$=0$．但$r^2=0$给出$t^4=-1$，此与$t^4\geqslant 0$相矛盾；$r^4-1=0$给出$r=\pm 1$、

$s=1$，$u+v=2s+1=8$；$2a^4=(s+1)s$ 给出 $a^2=1$，$u=2a^2=2$，$v=3-u=1$，$m^2=2uv=4$，$x+1=2m^2=8$，$x=7$；$y^2=(x+1)(x^2++1)$ 给出$y=\pm 20$。又因为$t^4+(r^2)^4=(r^4+1)^2$无解，故当m为偶数时，原方程只有解$x=7$，$y=\pm 20$。

综上所述，方程

$$1+x+x^2+x^3=y^2$$

只有解$x=-1$、$y=0$；$x=0$、$y=\pm 1$；

$x=1$、$y=\pm 2$；$x=7$、$y=\pm 20$。

习题7 证明不定方程

$$m\operatorname{arctg}\frac{1}{x}+n\operatorname{arctg}\frac{1}{y}=k\frac{\pi}{4},$$

1) 当$k=1$，$m=1$，$n=1$时有整数解：

$x=2$、$y=3$；$x=3$、$y=2$。

2) 当$k=1$、$m=2$、$n=-1$时有整数解：

$x=y=1$；$x=2$、$y=7$；$x=3$、$y=-7$。

3) 当$k=1$、$m=2$、$n=1$时有整数解：

$x=1$、$y=-1$；$x=2$、$y=-7$；$x=3$、$y=7$。

4) 当$k=1$、$m=4$、$n=-1$时有整数解：

$x=5$、$y=239$。

试利用最后一解以计划π之值准确至十万分之一。

证.（一） $\operatorname{arctg}\frac{1}{x}+\operatorname{arctg}\frac{1}{y}=\frac{\pi}{4}$的解为$x=2$、$y=3$；$x=3$，$y=2$。

由

$$\operatorname{tg}\left(\operatorname{arctg}\frac{1}{x}+\operatorname{arctg}\frac{1}{y}\right)=\operatorname{tg}\frac{\pi}{4}$$

有

$$x+y=xy-1.$$

i) 如果x偶、y偶，$x+y=xy-1$给出$0\equiv -1 \pmod 2$，此不可能。

ii) 如果x奇、y奇，设$x=2x_1+1$、$y=2y_1+1$、$x+y=xy-1$给出$2x_1y_1=1$，此也不可能。

iii) 如果x偶、y奇，设$x=2x_1$、$y=2y_1+1$、$x+y=xy-1$变成

$y_1(2x_1-1)=1$，此时有解$x_1=y_1=1$，从而$x=2$，$y=3$。

Ⅳ）如果x奇、y偶，同iii）可得$x=3$、$y=2$。

所以$k=m=n=1$时，原方程有解

$$x=2、y=3；\ x=3、y=2.$$

（二） $2\operatorname{arctg}\frac{1}{x}-\operatorname{arctg}\frac{1}{y}=\frac{\pi}{4}$的解为$x=y=1$；$x=2$、$y=7$；$x=3$、$y=-7$。

由
$$\operatorname{tg}\left(2\operatorname{arctg}\frac{1}{x}-\operatorname{arctg}\frac{1}{y}\right)=\operatorname{tg}\frac{\pi}{4}$$

有
$$\frac{\frac{2x}{x^2-1}-\frac{1}{y}}{1+\frac{2x}{x^2-1}\cdot\frac{1}{y}}=1,$$

整理得
$$y=\frac{-x^2-2x+1}{x^2-2x-1}=-1-\frac{4x}{x^2-2x-1}\tag{1}$$

i）当$x\geqslant 7$时，$x^2-2x-1>4x>0$，$x^2-2x-1\nmid 4x$，y非整数，此时无解。

ii）当$x\leqslant -3$时，$x^2-2x-1>|4x|$，$x^2-2x-1\nmid 4x$，y为非整数，此时也无解。

iii）当$x=1$时，由（1）得$y=1$，验证后知道$x=y=1$原方程的解；$x=2$时，由（1）由$y=7$，验证后知道$x=2$、$y=7$为原方程的解；$x=3$时，由（1）得$y=-7$，验证后知道$x=3$、$y=-7$为原方程的解。对于-3和7之间的其它x，可直接验证不是方程的解。故当$k=1$、$m=2$、$n=-1$时，原方程的解为$x=y=1$；$x=2$、$y=7$；$x=3$、$y=-7$。

（三）$2\operatorname{arctg}\frac{1}{x}+\operatorname{arctg}\frac{1}{y}=\frac{\pi}{4}$的解为$x=1$、$y=-1$；$x=2$、$y==-7$；$x=3$、$y=7$。

由
$$\operatorname{tg}\left(2\operatorname{arctg}\frac{1}{x}+\operatorname{arctg}\frac{1}{y}\right)=\operatorname{tg}\frac{\pi}{4}$$

有

$$\frac{\dfrac{2x}{x^2-1}+\dfrac{1}{y}}{1-\dfrac{2x}{x^2-1}\cdot\dfrac{1}{y}}=1,$$

整理得 $y=\dfrac{x^2+2x-1}{x^2-2x-1}=1+\dfrac{4x}{x^2-2x-1}$ （2）

i）由（二）可知，当$x\leqslant-3$、$x\geqslant7$时，原方程无解。

ii）当$x=1$时，由（2）得$y=-1$，验证后知道$x=1$、$y=-1$是原方程的解；$x=2$时，由（2）得$y=-7$，验证后知道$x=2$、$y=-7$是原方程的解；$x=3$时，由（2）得$y=7$，验证后知道$x=3$、$y=7$是原方程的解。-3和7之间的其它x，可直接验证不是原方程的解。故当$k=1$、$m=2$、$n=1$时，原方程的解为$x=1$、$y=-1$；$x=2$、$y=-7$；$x=3$、$y=7$。

（四） $4\operatorname{arctg}\dfrac{1}{x}-\operatorname{arctg}\dfrac{1}{y}=\dfrac{\pi}{4}$的解为$x=5$、$y=239$.

由

$$\operatorname{tg}\left(4\operatorname{arctg}\frac{1}{x}-\operatorname{arctg}\frac{1}{y}\right)=\operatorname{tg}\frac{\pi}{4}$$

有

$$\frac{\dfrac{4x(x^2-1)}{(x^2-1)^2-4x^2}-\dfrac{1}{y}}{1+\dfrac{4x(x^2-1)}{(x^2-1)^2-4x^2}\cdot\dfrac{1}{y}}=1,$$

整理得

$$y=\frac{x^4+4x^3-6x^2-4x+1}{-x^4+4x^3+6x^2-4x-1}=-1-\frac{8x^3-8x}{x^4-4x^3-6x^2+4x+1} \quad （3）$$

i）当$x\geqslant13$时

$$x^4-4x^3-6x^2+4x+1>8x^3-8x>0$$

$$x^4-4x^3-6x^2+4x+1\nmid 8x^3-8x$$

此时y非整数，故原方程无解。

ii）当$x\leqslant-6$时

$$x^4-4x^3-6x^2+4x+1>|8x^3-8x|$$

$$x^4-4x^3-6x^2+4x+1\nmid 8x^3-8x$$

此时y也非整数，故原方程无解。

iii）当$x=5$时，由（8）得$y=239$，验证后知道$x=5$、$y=239$是原方程的解。对于-6和13之间的其它x，可直接验证不是原方程的解。故当$k=1$、$m=4$、$n=-1$时，原方程的解为$x=5$、$y=239$。

下面利用最后一式，即$4\operatorname{arctg}\frac{1}{5}-\operatorname{arctg}\frac{1}{239}=\frac{\pi}{4}$来计算$\pi$。

$$\frac{\pi}{4}=4\operatorname{arctg}\frac{1}{5}-\operatorname{arctg}\frac{1}{239}$$

$$=4\left[\frac{1}{5}-\frac{1}{3}\cdot\frac{1}{5^3}+\frac{1}{5}\cdot\frac{1}{5^5}-\frac{1}{7}\cdot\frac{1}{5^7}+r_7\left(\frac{1}{5}\right)\right]-\left[\frac{1}{239}+\right.$$

$$\left.+r_1\left(\frac{1}{239}\right)\right]$$

由交错级数对误差的估计得

$$\left|4r_7\left(\frac{1}{5}\right)-r_1\left(\frac{1}{239}\right)\right|<\frac{4}{9\cdot5^9}+\frac{1}{3\cdot239^3}<0.5\cdot10^{-6}$$

用四舍五入法对其它各项计算如下：

$\frac{1}{5}=0.2000000$	$\frac{1}{3\cdot5^3}\approx0.0026667$
$\frac{1}{5\cdot5^5}=0.0000640$	$\frac{1}{7\cdot5^7}\approx0.0000018$
$+0.2000640$	-0.0026683

又因为 $\frac{1}{239}\approx0.0041841$

于是 $\pi\approx4\{4[0.2000640-0.0026685]-0.0041841\}$

$=3.1415916$

因此$\pi\approx3.14159$，而误差为

$$|\pi-3.14159|<4\times0.5\times10^{-6}+4\times4\times2\times0.5\times10^{-7}$$
$$+4\times0.5\times10^{-7}+1.6\times10^{-6}$$
$$<5.4\times10^{-6}<10^{-5}.$$

说明：原题当$k=1$、$m=1$、$n=1$时，只有一组解$x=2$、$y=3$；当$k=1$、$m=2$、$n=-1$时，只有一组解$x=2$；$y=7$；当$k=1$、$m=2$、$n=1$时，只有一组解$x=3$、$y=7$。但从（一）、（二）、（三）的证明可以看出原题有误，因为：

当$k=1$、$m=1$、$n=1$时，其整数解为$x=2$、$y=3$；$x=3$、$y=2$。

当$k=1$、$m=2$、$n=-1$时，其整数解为$x=2$、$y=7$；$x=y=1$；$x=3$、$y=-7$。

当$k=1$、$m=2$、$n=1$时，其整数解为$x=3$、$y=7$；$x=1$、$y=-1$；$x=2$、$y=-7$。

第十二章　二元二次型

一、提　　要

定义　对固定的整数a、b、c，二次齐次多项式$F=F(x, y)=ax^2+bxy+cy^2$，称为二元二次型，或简称二次型，以$\{a, b, c\}$表示。$d=b^2-4ac$称为F的判别式。

定理1　F可分为两个整系数一次式的乘积的充分必要条件是d为平方数。

定义　若有一整系数变换

$x=rX+sY$，$y=tX+uY$，$ru-st=1$。变$F(x, y)$为$G(X, Y)$，则称F与G相似，用$F\sim G$表示。或称F经$\begin{pmatrix} r & s \\ t & u \end{pmatrix}$变为$G$。

定理 2　如果$F\sim G$，则它们的判别式相等。

定义　按相似可将判别式为d的诸型分为若干类，同一类的诸型都相似，不同类的诸型绝对不相似。

定理 3　类数有限。

定理 4　判别式为d的定正型的类数等于适合

$$b^2-4ac=d,\quad \begin{cases} -a<b\leqslant a<c \\ \text{或 } 0\leqslant b\leqslant a=c \end{cases} \tag{1}$$

的整数组a、b、c的组数。

定义　适合（1）的二次型称为已化型。

定义　设$d\equiv 0$或$1\pmod 4$且非平方数，$m>0$。Kronecker符号$\left(\frac{d}{m}\right)$定义如下：

$$\left(\frac{d}{p}\right)=0,\qquad 若\quad p\mid d$$

$$\left(\frac{d}{2}\right)=\begin{cases}1, & 若d\equiv 1\pmod 8\\ -1, & 若d\equiv 5\pmod 8\end{cases}$$

$$\left(\frac{d}{p}\right)=\text{Legendre符号（}p\text{为奇素数，}p\nmid d\text{)}$$

$$若m=\prod_{r=1}^{v} p_r\text{，}p_r\text{ 为素数，则}$$

$$\left(\frac{d}{m}\right)=\prod_{r=1}^{v}\left(\frac{d}{p_r}\right).$$

定理5　若$m>0$，$(m、d)=1$，则Kronecker符号

$$\left(\frac{d}{m}\right)=\begin{cases}\left(\frac{m}{|d|}\right), & 当d为奇数时\\ \left(\frac{2}{m}\right)^b(-1)^{\frac{u-1}{2}\cdot\frac{m-1}{2}}\left(\frac{m}{|u|}\right), & 当d=\end{cases}$$

$2^b u$，$2\nmid u$时

此处$\left(\frac{m}{|d|}\right)$、$\left(\frac{2}{m}\right)$、$\left(\frac{m}{|u|}\right)$全为Jacobi符号.

定理6　Kronecker符号$\left(\frac{d}{m}\right)$为模$|d|$的实特征.

定理7　设$m>0$、$n>0$、$m\equiv -n\ (\bmod |d|)$，则

$$\left(\frac{d}{m}\right)=\begin{cases}\left(\frac{d}{n}\right), & 若d>0\\ -\left(\frac{d}{n}\right), & 若d<0.\end{cases}$$

定理8 设$k>0$，$(d, k)=1$. 同余式

$$x^2\equiv d(\bmod 4k)$$

的解数为$2\sum_{f\,k}\left(\frac{d}{f}\right)$. 此处$f$过$k$的所有无平方因子的正因子.

定义 若$(a, b, c)=1$，则称$\{a, b, c\}$为原型；若$(a, b, c)=g>1$，则称$\{a, b, c\}$为非原型.

定义 用$h(d)$表示以d为判别式的原型的类数.

定理9 以d为判别式的型的类数等于

$$\sum_{\substack{g^2\mid d\\ g>0}} h\left(\frac{d}{g^2}\right).$$

定理10 设$k>0$，$(k, d)=1$. 命$\psi(k)$表诸等式

$$k=F_1(x, y),\ \cdots,\ k=F_{h(d)}(x, y)$$

的原解个数的总和，则

$$\psi(k)=w\sum_{n\mid k}\left(\frac{d}{n}\right).$$

其中

$$w=\begin{cases}2, & 若d<-4\\ 4, & 若d=-4\\ 6, & 若d=-3.\end{cases}$$

定理11 $x^2+y^2=k$的解数等于四倍于k的因数$\equiv 1(\bmod 4)$的个数，减去k的因数$\equiv 3(\bmod 4)$的个数.

定义 命q为一素数. 若有一整系数变换

$$x=rX+sY,\quad y=tX+uY,\quad (ru-st,\ q)=1$$

使 $ax^2+bxy+cy^2\equiv a_1X^2+b_1XY+c_1Y^2 \pmod q$，

则称二次型 $\{a,\ b,\ c\}$ 与 $\{a_1,\ b_1,\ c_1\}$ mod q相似。

定理12 $p>2$．二次型 $\{a,\ b,\ c\}$ 与 $\{a_1,\ b_1,\ c_1\}$ 的判别式各为d、d_1，且$p|d$，$p|d_1$．则二次型 $\{a,\ b,\ c\}$ 与 $\{a_1,\ b_1,\ c_1\}$ mod p相似的充分必要条件是

$$\left(\frac{k}{p}\right)=\left(\frac{k_1}{p}\right).$$

其中k、k_1各为任何能经 $\{a,\ b,\ c\}$，$\{a_1,\ b_1,\ c_1\}$ 表出，且适合 $(k,\ d)=(k_1,\ d)=1$ 的整数。

定义 命p_1，…，p_s为d的奇素因子。若 $(k,\ 2d)=1$ 且k可经$F(x,\ y)$ 表出，则称

$$\left(\frac{k}{p_t}\right),\ \delta(k),\ \varepsilon(k),\ \delta(k)\varepsilon(k)$$

为$F(x,\ y)$ 的特征系。其中

$$\delta(k)=(-1)^{\frac{k-1}{2}},\qquad 若\frac{d}{4}\equiv 0 或 3 \pmod 4；$$

$$\varepsilon(k)=(-1)^{\frac{k^2-1}{8}},\qquad 若\frac{d}{4}\equiv 0 或 2 \pmod 8；$$

$$\delta(k)\varepsilon(k)=(-1)^{\frac{k-1}{2}+\frac{k^2-1}{8}},\quad 若\frac{d}{4}\equiv 0 或 6 \pmod 8。$$

定义 若两个有相同判别式d的二次型类的每个特征值都相等，则称它们属于同一族。

定理13 每一族中所含类数相等。

定义 用$K(d)$表级数，$K(d)=\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\frac{1}{n}$.

定理14

$$h(d)=\begin{cases}\frac{w\sqrt{|d|}}{2\pi}K(d), & 若 d<0\\ \frac{\sqrt{d}}{\log\varepsilon}K(d), & 若 d>0\end{cases}$$

其中

$$w=\begin{cases}2, & d<-4\\ 4, & d=-4\\ 6, & d=-3\end{cases}, \quad \varepsilon=\frac{x_0+y_0\sqrt{d}}{2}$$

$x_0+y_0\sqrt{d}$ 是$x^2-dy^2=4$的基本解.

定义 如果判别式d不含奇素数的平方因子，且d或为奇数，或$\equiv 8 \pmod{16}$，或$\equiv 12 \pmod{16}$，则称d为基本判别式.

定理15 设d为一负的基本判别式，则

$$h(d)=\frac{w}{2\left(2-\left(\frac{d}{2}\right)\right)}\sum_{r=1}^{\left[\frac{|d|}{2}\right]}\left(\frac{d}{r}\right).$$

定理16 命$d\geqslant 5$，则

$$K(d)<\frac{1}{2}\log d+1.$$

定理17 $\log\varepsilon<\sqrt{d}\left(\frac{1}{2}\log d+1\right)$.

定理18 $\log\varepsilon<\sqrt{d}\log d$.

定理19 若d为一判别式，则

$$\lim_{d\to-\infty}\frac{\log h(d)}{\log|d|}=\frac{1}{2}$$

$$\lim_{d\to\infty}\frac{\log(h(d)\log e)}{\log d}=\frac{1}{2}.$$

二、题　　解

§2　类数有限

习题1　下表给出 $0<-d\leqslant 20$之所有的已化型。

d	-3	-4	-7	-8	-11	-12		-15		-16		-19	-20	
a	1	1	1	1	1	1	2	1	2	1	2	1	1	2
b	1	0	1	0	1	0	2	1	1	0	0	1	0	2
c	1	1	2	2	3	3	2	4	2	4	2	5	5	3

证：因为

当$d=-1$时，$b^2-4ac=-1$给出$1\equiv-1\pmod 4$；

当$d=-2$时，$b^2-4ac=-2$给出$0\equiv-2\pmod 4$；

当$d=-5$时，$b^2-4ac=-5$给出$1\equiv-5\pmod 4$；

当$d=-6$时，$b^2-4ac=-6$给出$0\equiv-6\pmod 4$；

当$d=-9$时，$b^2-4ac=-9$给出$1\equiv-9\pmod 4$；

当$d=-10$时，$b^2-4ac=-10$给出$0\equiv-10\pmod 4$；

当$d=-13$时，$b^2-4ac=-13$给出$1\equiv-13\pmod 4$；

当$d=-14$时，$b^2-4ac=-14$给出$0\equiv-14\pmod 4$；

当$d=-17$时，$b^2-4ac=-17$给出$1\equiv-17\pmod 4$；

当$d=-18$时，$b^2-4ac=-18$给出$0\equiv-18\pmod 4$.

所以，当$0<-d\leqslant 20$时的所有已化型只能在$d=-3$、-4、-7、-8、-11、-12、-15、-16、-19、-20的时候存在（即上表中所列的d的值）．下面给出$d=-20$时的两个已化型

$$\{1,\ 0,\ 5\},\ \{2,\ 2,\ 3\}$$

的证明（上表中所列的其余部分，用完全相同的方法可以证明）．

要证明$d=-20$时只有两个已化型$\{1,\ 0,\ 5\}$、$\{2,\ 2,\ 3\}$，由定义，只须证明$b^2-4ac=-20$合条件

$$\begin{cases}-a<b\leqslant a<c\\ \text{或 } 0\leqslant b\leqslant a=c\end{cases}\text{的整数解}$$

$$\{a,\ b,\ c\}=\{1,\ 0,\ 5\},\ \{2,\ 2,\ 3\}\text{即可.}$$

（一）先考虑在条件$0\leqslant b\leqslant a=c$下，$b^2-4ac=-20$的整数解．

1） 当$0=b<a=c$时，$b^2-4ac=-20$给出$a^2=5$，矛盾．

2） 当$0=b=a=c$时，$b^2-4ac=-20$给出$0=-20$，矛盾．

3） 当$0<b<a=c$时，由于b偶，并且$a>0$，$b^2-4ac=b^2-4a^2=-20$给出$(b+2a)\cdot(b-2a)=-20$，$b+2a=10$，$b-2a=-2$，$b=4$，$a=3$，与$b<a$矛盾．

4） 当$0<b=a=c$时，$b^2-4ac=-20$给出$3b^2=20$，矛盾．

（二）再考虑在条件$-a<b\leqslant a<c$之下，$b^2-4ac=-20$的整数解．

1） 当$-a<b=a<c$时，$b^2-4ac=-20$给出$b(b-4c)=-20$，又因为b偶且$c>0$，从而$b-4c=-10$，$b=2$，$c=3$，$a=2$，$b=2$，与它对应的一个已化型为$\{2, 2, 3\}$.

2） 当$-a<b<c$时，$b^2-4ac=-20$给出$-20=b^2-4ac<a^2-4a^2=-3a^2$，$3a^2<20$。又因为$a>0$，故$a=1, 2$。$a=1$时，由$-1<b<1$有$b=0$，从而$c=5$，与它对应的一个已化型为$\{1, 0, 5\}$；$a=2$时，$-2<b<2$给出$b=-1, 0, 1$。而$b=\pm1$时，给出$8c=21$，$b=0$时又有$8c=20$。这些都不可能。

由（一）、（二）可知$d=-20$时，只有表中所列的两个已化型

$$\{1, 0, 5\}, \{2, 2, 3\}.$$

下面再给出一种证法。先利用$0<a\leqslant\sqrt{\frac{|d|}{3}}$定出$a$的限。

因为$\sqrt{\frac{|d|}{3}}=\sqrt{\frac{20}{3}}=\frac{2\sqrt{15}}{3}<\frac{2\sqrt{16}}{3}=\frac{8}{3}<3$，所以$a=1, 2$.

（一）当$0\leqslant b\leqslant a=c$时

1）如果$a=1$，则$c=1$，$b=0, 1$.此时$b^2-4ac=-4, -3$，故$b^2-4ac\neq-20$。

2）如果$a=2$，则$c=2$，$b=0, 1, 2$，此时$b^2-4ac=-16, -15, -12$，故$b^2-4ac\neq-20$。

（二）当$-a<b\leqslant a<c$时

1）如果$a=1$，则$b=0, 1$，从$b^2-4ac=-20$得$c=5$，

$\frac{21}{4}$，故此时只有一个已化型 $\left\{1,\ 0,\ 5\right\}$.

2）如果$a=2$，则$b=-1$，0，1，2，从$b^2-4ac=-20$得$c=\frac{21}{8}$，$\frac{5}{2}$，$\frac{21}{8}$，3，因此只有一个已化型 $\left\{2,\ 2,\ 3\right\}$.

此题的第二种证明方法，是由柯召教授给出的．第二种证法比第一种证法简单，特别是当d的绝对值较大的时候．

习题 2　证明$d=-48$时有四个已化型：$\left\{1,\ 0,\ 12\right\}$，$\left\{2,\ 0,\ 6\right\}$，$\left\{3,\ 0,\ 4\right\}$，$\left\{4,\ 4,\ 4\right\}$.

证：（一）先研究在条件 $0\leqslant b\leqslant a=c$之下，$b^2-4ac=-48$的整数解．

1）当$0=b<a=c$时，$b^2-4ac=-48$变为$4a^2=48$，$a^2=12$，此不可能．

2）当$0=b=a=c$时，$b^2-4ac=-48$变为$0=-48$，矛盾．

3）当$0<b<a=c$时，$b^2-4ac=-48$给出$(b+2a)(b-2a)=-48$，再由b偶、$a>0$可得

$$\begin{cases}b+2a=2^3\cdot 3\\ b-2a=-2\end{cases}\qquad (\text{I})$$

或

$$\begin{cases}b+2a=2^2\cdot 3\\ b-2a=-2^2\end{cases}\qquad (\text{II})$$

或

$$\begin{cases}b+2a=2^3\\ b-2a=-2\cdot 3\end{cases}\qquad (\text{III})$$

由（I）有$b=11$，$2a=13$，矛盾；

由（II）有$b=4$，$a=4$，$c=4$，此时对应一个已化型

$$\{4,\ 4,\ 4\}$$

由（Ⅲ）有$b=1$，$2a=7$，矛盾。

4）当$0<b=a=c$时，$b^2-4ac=-48$变为$-3b^2=-48$，$b^2=16$，$b=4$，$a=c=4$，此时也与已化型$\{4,\ 4,\ 4\}$对应。

（二）再研究在条件$-a<b\leqslant a<c$之下，$b^2-4ac=-48$的整数解。

1）当$-a<b=a<c$时，$b^2-4ac=-48$变为$b^2-4bc=-48$，$b(b-4c)=-48$。由于b偶且$c>0$，因此$b(b-4c)=-48$给出

$$\begin{cases}b=2^3\cdot 3\\ b-4c=-2\end{cases}\qquad〈Ⅰ〉$$

或

$$\begin{cases}b=2^2\cdot 3\\ b-4c=-2^2\end{cases}\qquad〈Ⅱ〉$$

或

$$\begin{cases}b=2^3\\ b-4c=-2\cdot 3\end{cases}\qquad〈Ⅲ〉$$

或

$$\begin{cases}b=2\\ b-4c=-2^3\cdot 3\end{cases}\qquad〈Ⅳ〉$$

或

$$\begin{cases}b=2^2\\ b-4c=-2^2\cdot 3\end{cases}\qquad〈Ⅴ〉$$

或

$$\begin{cases}b=2\cdot 3\\ b-4c=-2^3\end{cases}\qquad〈Ⅵ〉$$

由〈Ⅰ〉有$b=24$，$4c=26$，矛盾；

由〈Ⅱ〉有$b=12$，$c=4$，此与$b<c$矛盾；

由〈Ⅲ〉有$b=8$，$4c=14$，矛盾；

由（Ⅳ）有$b=2$，$4c=26$，矛盾；

由（Ⅴ）有$b=4$，$a=c=4$，此时仍然对应于已化型$\{4,4,4\}$；

由（Ⅵ）有$b=6$，$4c=14$，矛盾。

2）当$-a<b<a<c$时，$b^2-4ac=-48$给出$-48=b^2-4ac<a^2-4a^2=-3a^2$，$3a^2<48$，$a^2<16$。又因为$a>0$，可得$a=1,2,3$。如果$a=1$，由$-1=-a<b<a=1$知道$b=0$，$c=12$，此时对应已化型$\{1,0,12\}$；

如果$a=2$，由$-2=-a<b<a=2$知道$b=-1,0,1$。对于$a=2$，$b=\pm1$，$b^2-4ac=-48$给出$8c=49$，矛盾；对于$a=2$，$b=0$，由$b^2-4ac=-48$给出$c=6$，与此相对应的一个已化型为$\{2,0,6\}$。

如果$a=3$，由$-3=-a<b<a=3$知道$b=-2,-1,0,1,2$。对于$a=3$，$b=\pm1$，$b^2-4ac=-48$给出$12c=49$，矛盾；对于$a=3$，$b=0$，$b^2-4ac=-48$给出$c=4$，与此相应的一个已化型是$\{3,0,4\}$；对于$a=3$，$b=\pm2$，又有$12c=52$，矛盾。

由（一）、（二）可知，$d=-48$时的确只有四个已化型：

$$\{1,0,12\},\ \{2,0,6\},\ \{3,0,4\},\ \{4,4,4\}.$$

下面再给出一种证法。

因为 $0<a\leqslant\sqrt{\dfrac{|d|}{3}}=\sqrt{\dfrac{48}{3}}=4$

所以$a=1$，2，3，4。

（一）当$0\leqslant b\leqslant a=c$时

1）如果$a=1$，则$c=1$，$b=0$，1，$b^2-4ac=-4$，-3，故$b^2-4ac\neq-48$。

2）如果$a=2$，则$c=2$，$b=0$，1，2，$b^2-4ac=-16$，-15，-12，故$b^2-4ac\neq-48$。

3）如果$a=3$，则$c=3$，$b=0$，1，2，3，$b^2-4ac=-36$，-35，-32，-27，故$b^2-4ac\neq-48$。

4）如果$a=4$，则$c=4$，$b=0$，1，2，3，4，$b^2-4ac=-64$，-63，-60，-55，-48，此时只得一个已化型$\{4,4,4\}$。

（二）当$-a<b\leqslant a<c$时

1）如果$a=1$，则$b=0$，1，由$b^2-4ac=-48$得$c=12$，$\frac{49}{4}$，此时得一个已化型$\{1,0,12\}$。

2）如果$a=2$，则$b=-1$，0，1，2，由$b^2-4ac=-48$得$c=\frac{49}{8}$，6，$\frac{49}{8}$，$\frac{13}{2}$，此时也只有一个已化型$\{2,0,6\}$。

3）如果$a=3$，则$b=-2$，-1，0，1，2，3，$c=\frac{13}{3}$，$\frac{49}{12}$，4，$\frac{49}{12}$，$\frac{13}{3}$，$\frac{19}{4}$，此时也只有一个已化型$\{3,0,4\}$。

4）如果$a=4$，则$b=-3$，-2，-1，0，1，2，3，4，$c=\frac{57}{16}$，$\frac{13}{4}$，$\frac{49}{16}$，3，$\frac{49}{16}$，$\frac{13}{4}$，$\frac{57}{16}$，4。再因$a=4$，$c=4$，

3 时，$a<c$不成立，所以此时没有已化型。

此题的第二种证明方法，是由柯召教授给出的，它比第一种证法简单得多。

§4 二次型表整数之表法数

习题1 若m为奇数，$x^2+2y^2=2^l m$之解数等于2σ，此处σ为m之因数$\equiv 1$或$3 \pmod 8$者之个数减去m之因数$\equiv 5$或$7 \pmod 8$者之个数。

证： $d=b^2-4ac=-8$，$h(d)=h(-8)$表示以$d=-8$为判别式的原型类数。由于$d=-8<0$、$a=1>0$、$F(x, y)=x^2+2y^2$为正定型，$h(-8)$就是方程$b^2-4ac=-8$合条件

$$\begin{cases} -a<b\leqslant a<c \\ \text{或 } 0\leqslant b\leqslant a=c \end{cases} \quad \text{且 } (a, b, c)=1$$

的解数，从而易证$h(-8)=1$。下边，设$k=2^l m$，对l行归纳法，证明$x^2+2y^2=k$的解数为$\psi(m)$（此处用到了提要中的定理10）。

因为 $$\psi(m)=w\sum_{n|m}\left(\frac{d}{n}\right)=2\sum_{n|m}\left(\frac{-8}{n}\right),$$

（当$d=-8$时，$w=2$）而Kronecker符号

$$\left(\frac{-8}{n}\right)=\begin{cases} 1, & \text{当 } n\equiv 1,\ 3 \pmod 8 \text{ 时} \\ 0, & \text{当 } (n, 8)>1 \text{ 时} \\ -1, & \text{当 } n\equiv 5,\ 7 \pmod 8 \text{ 时} \end{cases} \qquad (1)$$

当$l=0$时，$x^2+2y^2=m$，$(m, d)=(m, -8)=1$。由定理10，$x^2+2y^2=m$的解数为$\psi(m)$。归纳假定$l=1, 2, \cdots, t$时，$x^2+2y^2=2^l m$的解数为$\psi(m)$。考虑方程$x^2+2y^2=2^{t+1}m$。显然，x、y全为偶数。设$x=2x_1$，$y=2y_1$，就有$x_1^2+2y_1^2=2^{t-1}m$。由归纳假定，$x_1^2+2y_1^2=2^{t-1}m$的解数为$\psi(m)$。注意到$x^2+2y^2=2^{t+1}m$的解数与$x_1^2+2y_1^2=2^{t-1}m$的解数

相同，因此，$x^2+2y^2=2^{t+1}m$的解数为$\psi(m)$，结论对于$l=t+1$时也成立。故$\psi(m)$为方程$x^2+2y^2=2^lm$的解数．由（1）便知方程$x^2+2y^2=2^lm$的解数等于2倍m的因数$\equiv 1$或3（mod 8）的个数，减去m的因数$\equiv 5$或7(mod 8）的个数。

习题 2 $k=x^2+xy+y^2$之解数为$6E(k)$。此$E(k)$为k中形如$3h+1$之因数之个数减去形如$3h+2$之因数之个数。

证：$d=-3$．同习题1一样，易证$h(d)=h(-3)=1$．设$k=3^sm$，$s\geqslant 0$，$3\nmid m$。下面对s行归纳法证明$x^2+xy+y^2=k$的解数为$\psi(k)$。由定理10有

$$\psi(k)=w\sum_{n|k}\left(\frac{d}{n}\right)=6\sum_{n|k}\left(\frac{-3}{n}\right)=6\sum_{n|k}\left(\frac{n}{|-3|}\right)$$

$$=6\sum_{n|k}\left(\frac{n}{3}\right),$$

（当$d=-3$时，$w=6$）并且Legendre符号

$$\left(\frac{n}{3}\right)=\begin{cases}1, & \text{当}n\text{形如}3h+1\text{时}\\ -1, & \text{当}n\text{形如}3h+2\text{时}\end{cases}$$

故　$\psi(k)=6E(k)$

当$s=0$时，$x^2+xy+y^2=k=m$。由定理10立得它的解数为$\psi(k)=6E(k)$。归纳假定$s=1$，2，…，t时结论都成立．当$s=t+1$时，$k=3^{t+1}m$。对$x^2+xy+y^2=3^{t+1}m$取模9得$x^2+xy+y^2\equiv 0 \pmod 9$），从而有$3|x$，$3|y$。设$x=3x_1$，$y=3y_1$，可得$x_1^2+x_1y_1+y_1^2=3^{t-1}m$。因此，$x^2+xy+y^2=3^{t+1}m$的解数与$x_1^2+x_1y_1+y_1^2=3^{t-1}m$的解数相同。由归纳假定知其解数为$\psi(3^{t-1}m)$．但是

$$\psi(3^{t-1}m)=6\sum_{n|3^{t-1}m}\left(\frac{-3}{n}\right)=6\sum_{n|3^{t+1}m}\left(\frac{-3}{n}\right)$$

$$=\psi(3^{t+1}m)$$

故方程$x^2+xy+y^2=3^{t+1}m$的解数也为$\psi(3^{t+1}m)=\psi(k)$，因此$s=t+1$时结论也成立。所以方程$k=x^2+xy+y^2$的解数为$6E(k)$。

习题 3 若m为奇数，则$x^2+3y^2=2^lm$之解数有三种情形：若l是奇数，则无解；若$l=0$，则解数为$2E(m)$；若l为正偶数，则解数为$6E(m)$。此处$E(m)$之定义如上。

证：（一）若l是奇数，则$x^2+3y^2=2^lm$无解。

i) $x^2+3y^2=2m$无解，否则$0\equiv 2 \pmod 4$。

ii) 如果对于任一奇数$l>1$，$x^2+3y^2=2^lm$可解，那么x、y一定同奇同偶。如果同奇，$x^2+3y^2=2^lm$给出$4\equiv 0 \pmod 8$。如果同偶，设$x=2x_1$、$y=2y_1$、$x^2+3y^2=2^lm$变为$x_1{}^2+3y_1{}^2=2^{l-2}m$，此即方程$x^2+3y^2=2^{l-2}m$可解。继续讨论下去就有$x^2+3y^2=2^{l-4}m$可解，…，方程$x^2+3y^2=2m$可解，与i）矛盾。

（二）若$l=0$，则$x^2+3y^2=2^lm=m$的解数为$2E(m)$。此时$d=-12$，易证$h(d)=h(-12)=1$。设$m=3^tm_1$，$t\geqslant 0$，$3\nmid m_1$。

i) 当$t=0$时，$m=m_1$，$(m,\ d)=(m_1,\ -12)=1$，$x^2+3y^2=m_1$的解数由定理10知道为$\psi(m_1)$。具体而言：

$$\psi(m_1)=w\sum_{n\mid m_1}\left(\frac{d}{n}\right)=2\sum_{n\mid m_1}\left(\frac{-12}{n}\right)$$

$$=2\sum_{n\mid m_1}\left(\frac{2^2\cdot(-3)}{n}\right)=2\sum_{n\mid m_1}\left(\frac{2}{n}\right)^2(-1)^{\frac{n-1}{2}\cdot\frac{-3-1}{2}}$$

$$\cdot\left(\frac{n}{|-3|}\right)=2\sum_{n\mid m_1}\left(\frac{n}{3}\right)=2E(m_1)=2E(m),$$

（当$d=-12$时，$w=2$）。

ii) 归纳假定$t=1,\ 2,\ \cdots,\ k$时结论成立。下面将证明x^2

$+3y^2=3^{k+1}m_1$ 的解数为 $2E(3^{k+1}m_1)$．由 $x^2+3y^2=3^{k+1}m_1$ 有 $3|x$，设 $x=3x_1$，$x^2+3y^2=3^{k+1}m_1$ 变成 $3x_1^2+y^2=3^km_1$，因此，$x^2+3y^2=3^km_1$ 与 $x^2+3y^2=3^{k+1}m_1$ 的解数是相同的，由归纳假定为 $2E(3^km_1)$．因此，下面只须证明 $E(3^{k+1}m_1)=E(3^km_1)$ 即可．注意到Kronecker 符号的一个性质：$(a,b)>1$，$\left(\frac{a}{b}\right)=0$，就有

$$E(3^km_1)=\sum_{n|3^km_1}\left(\frac{-12}{n}\right)=\sum_{n|3^{k+1}m_1}\left(\frac{-12}{n}\right)$$

$$=E(3^{k+1}m_1)．$$

（三）若 l 为正偶数，则 $x^2+3y^2=2^lm$ 的解数为 $6E(m)$．

i）$x^2+3y^2=2^l\cdot3^tm_1$，$(6,m_1)=1$，$t\geqslant0$ 的解数与 $x^2+3y^2=2^lm_1$ 的解数相同。当 $t=0$ 时，上述断语正确。对于 $t\geqslant1$，只须证明 $x^2+3y^2=2^l\cdot3^tm_1$ 的解数与 $x^2+3y^2=2^l\cdot3^{t-1}m_1$ 的解数相同即可。

由 $x^2+3y^2=2^l\cdot3^tm_1$ 知 $3|x$，设 $x=3x_1$，$x^2+3y^2=2^l\cdot3^tm_1$ 变为 $3x_1^2+y^2=2^l\cdot3^{t-1}m_1$，此即如果 $x^2+3y^2=2^l\cdot3^tm_1$ 有一解，那么方程 $x^2+3y^2=2^l\cdot3^{t-1}m_1$ 也有一解与之对应；反过来，若 $x^2+3y^2=2^l\cdot3^{t-1}m_1$，就有 $3x^2+(3y)^2=2^l\cdot3^tm_1$，即 $x^2+3y^2=2^l\cdot3^{t-1}m_1$ 有一解，那么 $x^2+3y^2=2^l\cdot3^tm_1$ 也有一解与之对应．故方程 $x^2+3y^2=2^l\cdot3^tm_1$ 的解数与 $x^2+3y^2=2^l\cdot3^{t-1}m_1$ 的解数相同。

由i）可知，要证明 $x^2+3y^2=2^lm$ 当 l 为正偶数时的解数为 $6E(m)$，只须证明 l 为正偶数且 $3\nmid m$ 时 $x^2+3y^2=2^lm$ 的解数为 $6E(m)$ 即可。下面对 l 行归纳法证明此点。

ii）设 $l=2r$，$r\geqslant1$，$3\nmid m$，$x^2+3y^2=2^lm$．当 $r=1$ 时，$x^2+3y^2=2^lm$ 变为 $x^2+3y^2=4m$。

(*a*) 如果$x\equiv y\equiv 0\pmod 2$，设$x=2x_1$，$y=2y_1$，就有$x_1^2+3y_1^2=m$，且$2\nmid(x_1, y_1)$．此时由于m奇且$3\nmid m$，就有$(m, d)=(m, -12)=1$．由定理10，方程$x_1^2+3y_1^2=m$的解数为

$$\psi(m)=w\sum_{n\mid m}\left(\frac{d}{n}\right)=2\sum_{n\mid m}\left(\frac{-12}{n}\right)$$

$$=2\sum_{n\mid m}\left(\frac{2^2\cdot(-3)}{n}\right)=2\sum_{n\mid m}\left(\frac{2}{n}\right)^2(-1)^{\frac{n-1}{2}\cdot\frac{-3-1}{2}}\cdot$$

$$\left(\frac{n}{|-3|}\right)=2\sum_{n\mid m}\left(\frac{n}{3}\right)=2E(m)$$

(*b*) 如果$x\equiv y\equiv 1\pmod 2$，因为$l^2\equiv d\pmod{4k}$即$l^2\equiv-12\pmod{4\cdot 4m}$的解数为$l^2\equiv-12\pmod{16}$的解数与$l^2\equiv-12\pmod m$的解数的乘积，$l^2\equiv-12\pmod{16}$的解为$l\equiv 2, 6, 10, 14\pmod{16}$，解数为4；而$l^2\equiv-12\pmod m$的解数为$\prod_{p\mid m}\left(1+\left(\frac{d}{p}\right)\right)$，因此$l^2\equiv-12\pmod{16m}$的解数为$4\prod_{p\mid m}\left(1+\left(\frac{d}{p}\right)\right)$．如果添加限制$0\leqslant l<2k$，那么解数就为$2\prod_{p\mid m}\left(1+\left(\frac{d}{p}\right)\right)$，从而方程$x^2+3y^2=4m$的既约原解数为：

$$2w\prod_{p\mid m}\left(1+\left(\frac{d}{p}\right)\right)=2w\sum_{f\mid m}\left(\frac{d}{f}\right)$$

（此处f为正且无平方因子）但当$d=-12$时，$w=2$，因此

$$2w\sum_{f\mid m}\left(\frac{d}{f}\right)=4\sum_{f\mid m}\left(\frac{-12}{f}\right)$$

故$x^2+3y^2=4m$的原解数为：

$$4\sum_{\substack{g^2 \mid 4m \\ 0<g\neq 2}}\sum_{f \mid \frac{4m}{g^2}}\left(\frac{-12}{f}\right)=4\sum_{\substack{g^2 \mid m \\ g>0}}\sum_{f \mid \frac{m}{g^2}}\left(\frac{-12}{f}\right)$$

$$=4\sum_{\substack{g^2 \mid m \\ g>0}}\sum_{f \mid \frac{m}{g^2}}\left(\frac{-12}{fq^2}\right)=4\sum_{n \mid m}\left(\frac{-12}{n}\right)$$

$$=4\sum_{n \mid m}\left(\frac{2^2\cdot(-3)}{n}\right)=4\sum_{n \mid m}\left(\frac{2}{n}\right)(-1)^{\frac{n-1}{2}\cdot\frac{-3-1}{2}}$$

$$\cdot\left(\frac{n}{|-3|}\right)=4\sum_{n \mid m}\left(\frac{n}{3}\right)=4E(m).$$

由(a)、(b)可知$x^2+3y^2=4m$的解数为$2E(m)+4E(m)=6E(m)$，故$r=1$时结论成立。设$r=2$，…，t时结论成立，即$x^2+3y^2=2^{2r}m$，$2\leqslant r\leqslant t$，$3\nmid m$的解数都为$6E(m)$。当$r=t+1$时，由$x^2+3y^2=2^{2(t+1)}m$可知x、y同奇偶。如果同奇，就有$4\equiv 0 \pmod 8$，此不可能；如果同偶，设$x=2x_1$，$y=2y_1$，$x^2+3y^2=2^{2(t+1)}m$变为$x_1^2+3y_1^2=2^{2t}m$，此即方程$x^2+3y^2=2^{2(t+1)}m$的解数与$x^2+3y^2=2^{2t}m$的解数相同。再由归纳假定知道就是$6E(m)$。

以上证明了$x^2+3y^2=2^lm$，l为正偶数且$3\nmid m$时，其解数为$6E(m)$，再由i）即得所证。

习题4　若m为奇数，则$x^2+3y^2=4m$有$E(m)$个正奇数解。

证：由习题3证明过程中的(b)可知，方程$x^2+3y^2=4m$的奇数解数为$4E(m)$，它包括x正y正、x正y负、x负y正、x负y负四种情形，故$x^2+3y^2=4m$的正奇数解数为$E(m)$。

习题5　若m为奇数，则$x^2+4y^2=2^km$之解数，当$k=0$时为$2E$，当$k=1$时为0，当$k\geqslant 2$时为$2E$，此处E为m之因子$\equiv 1 \pmod 4$者之个数减去m之因子$\equiv 3 \pmod 4$者之个

数。

证： 当$k=1$时，$x^2+4y^2=2^k m$变形为$x^2+4y^2=2m$，但x为偶数时$x^2+4y^2=2m$给出$0\equiv 2 \pmod 4$，故此种情无形解。

当$k=0$或$k\geqslant 2$时，设$y_1=2y$，$x^2+4y^2=2^k m$变为$x^2+y_1{}^2=2^k m$。熟知$X^2+Y^2=2^k m$的解数为$4\sum\limits_{n\mid 2^k m}\left(\frac{-4}{n}\right)$，故$x^2+4y^2=2^k m$的解数为$2\sum\limits_{n\mid 2^k m}\left(\frac{-4}{n}\right)$。

但当$n\equiv 1 \pmod 4$，$(n,\ 4)>1$，$n\equiv 3 \pmod 4$时，$\left(\frac{-4}{n}\right)$分别为1，0，$-1$，此即$\sum\limits_{n\mid 2^k m}\left(\frac{-4}{n}\right)=E(m)$。

从而当$k=0$或$k\geqslant 2$时，$x^2+4y^2=2^k m$的解数为$2E(m)$。

又：原题中定义E为m之素因子$\equiv 1 \pmod 4$者之个数减去k之因子$\equiv 3 \pmod 4$者之个数。其中"素因子"应改为"因子"，"k"应为"m"。

习题6 用$e(n)$记n之因子中$\equiv 1,\ 2,\ 4 \pmod 7$者之个数减去$\equiv 3,\ 5,\ 6 \pmod 7$者之个数所得之差，则$0<n=x^2+xy+2y^2$之解数为$2e(n)$。

证： 此时$d=-7$，$w=2$且$h(-7)=1$。设$n=7^s n_1$，$s\geqslant 0$，$7\nmid n_1$。

i）当$s=0$时，$(n,\ d)=(n_1,\ -7)=1$。由定理10，此种情形解数为

$$2\sum_{\substack{g^2\mid n_1\\ g>0}}\sum_{f\mid \frac{n_1}{g^2}}\left(\frac{-7}{f}\right)=2\sum_{\substack{g^2\mid n_1\\ g>0}}\sum_{f\mid \frac{n_1}{g^2}}\left(\frac{-7}{fq^2}\right)$$

$$= 2\sum_{m \mid n}\left(\frac{-7}{m}\right)$$

其中f为正且无平方因子.

又因 $\left(\frac{-7}{m}\right)=\begin{cases}\left(\frac{m}{7}\right) & 当\ (m,\ 7)=1\ 时\\ 0, & 当\ (m,\ 7)>1\ 时\end{cases}$

有 $\left(\frac{-7}{m}\right)=\begin{cases}1, & 当 m\equiv 1,\ 2,\ 4 \pmod 7 时\\ 0, & 当\ (m,\ 7)>1\ 时\\ -1, & 当 m\equiv 3,\ 5,\ 6 \pmod 7 时\end{cases}$

从而 $\sum_{m \mid n_1}\left(\frac{-7}{m}\right)=e(n_1)=e(n)$

此即$s=0$时方程的解数为$2e(n)$.

ii) 当$s\geqslant 1$时. 下面对s行归纳法证明$0<n=x^2+xy+2y^2$的解数为$2e(n)$. $s=1$时, $n=7n_1$, $l^2\equiv -7 \pmod 4$ 有解$l\equiv 1,\ 3 \pmod 4$, 解数为2; $l^2\equiv -7 \pmod{7n_1}$ 的解数为$\prod_{p \mid 7n_1}\left(1+\left(\frac{-7}{p}\right)\right)=\sum_{f \mid 7n_1}\left(\frac{-7}{f}\right)$. 因此,

$$l^2\equiv -7 \pmod{4\cdot 7n_1},\quad 0\leqslant l<2\cdot 7n_1$$

的解数为$\sum_{f \mid 7n_1}\left(\frac{-7}{f}\right)$. 方程$x^2+xy+2y^2=7n_1$的既约原解数为

$$w\sum_{f \mid 7n_1}\left(\frac{-7}{f}\right)=2\sum_{f \mid 7n_1}\left(\frac{-7}{f}\right)$$

从而解数为 $$2\sum_{\substack{g^2 \mid 7n_1\\ g<0}}\ \sum_{f \mid \frac{7n_1}{g^2}}\left(\frac{-7}{f}\right)$$

$$=2\left(\sum_{\substack{g^2 \mid n_1\\ g>0}}\ \sum_{f \mid \frac{n_1}{g^2}}\left(\frac{-7}{f}\right)+\sum_{\substack{g^2 \mid n_1\\ g>0}}\ \sum_{f \mid \frac{n_1}{g^2}}\left(\frac{-7}{7f}\right)\right)$$

$$= 2\sum_{\substack{g^2 \mid n_1 \\ g>0}} \sum_{f \mid \frac{n_1}{g^2}} \left(\frac{-7}{f}\right) = 2\sum_{m \mid n_1} \left(\frac{-7}{m}\right)$$

$$= 2\sum_{m \mid n} \left(\frac{-7}{m}\right) = 2e(n).$$

故$s=1$时结论成立。设$s=2$，…，t时结论亦成立，即$x^2+xy+2y^2=7^s n_1$，$2\leqslant s\leqslant t$的解数为$2e(n)$。对于$s=t+1$，用与上面相同的方法可证其解数为

$$2\sum_{\substack{g^2 \mid 7^{t+1}n_1 \\ g>0}} \sum_{f \mid \frac{7^{t+1}n_1}{g^2}} \left(\frac{-7}{f}\right)$$

又因
$$\sum_{\substack{g^2 \mid 7^{t+1}n_1 \\ g>0}} \sum_{f \mid \frac{7^{t+1}n_1}{g^2}} \left(\frac{-7}{f}\right) = \sum_{\substack{g^2 \mid 7^{t}n_1 \\ g>0}} \sum_{f \mid \frac{7^{t}n_1}{g^2}} \left(\frac{-7}{f}\right) + \sum_{\substack{g^2 \mid n_1 \\ g>0}} \sum_{f \mid \frac{n_1}{g^2}} \left(\frac{-7}{7^{t+1}f}\right),$$

且
$$\sum_{\substack{g^2 \mid n_1 \\ g>0}} \sum_{f \mid \frac{n_1}{g^2}} \left(\frac{-7}{7^{t+1}g^2}\right) = 0$$

再由归纳假定
$$\sum_{\substack{g^2 \mid 7^{t}n_1 \\ g>0}} \sum_{f \mid \frac{7^{t}n_1}{g^2}} \left(\frac{-7}{f}\right) = e(n)$$

立刻可以得到$x^2+xy+2y^2=7^{t+1}n_1$的解数为$2e(n)$，即结论对于$s=t+1$时也成立。由i)、ii)便知$0<n=x^2+xy+2y^2$的解数的确是$2e(n)$。

习题7　若m为奇数，则$e(2^a m)=(a+1)\cdot e(m)$。若$3\nmid t$，则当b为奇数时，$e(3^b t)=0$。而当b为偶数时，$e(3^b t)=e(t)$。

证： i）用归纳法证明，当m为奇数时，

$$e(2^a m)=(a+1)e(m).$$

当$a=0$时，显然有$e(2^a m)=(a+1)e(m)$。设$a=t$时结论成立。当$a=t+1$时

$$e(2^a m)=e(2^{t+1}m)=\sum_{n\mid 2^{t+1}m}\left(\frac{-7}{n}\right)$$

$$=\sum_{n\mid 2^t m}\left(\frac{-7}{n}\right)+\sum_{n\mid m}\left(\frac{-7}{2^{t+1}n}\right).$$

由归纳假定 $\sum_{n\mid 2^t m}\left(\frac{-7}{n}\right)=(t+1)e(m)$

且$\left(\frac{-7}{2}\right)=1$，从而就有

$$\sum_{n\mid m}\left(\frac{-7}{2^{t+1}n}\right)=\sum_{n\mid m}\left(\frac{-7}{2}\right)^{t+1}\left(\frac{-7}{n}\right)$$

$$=\sum_{n\mid m}\left(\frac{-7}{n}\right)=e(m),$$

故 $e(2^a m)=(t+1)e(m)+e(m)=(t+2)e(m)$。此即结论对于$a=t+1$时也成立。故当$m$为奇数时，总有

$$e(2^a m)=(a+1)e(m).$$

ii）再证若$3\nmid t$，则当b为奇数时，$e(3^b t)=0$。

因为 $$e(3^b t)=\sum_{n\mid 3^b t}\left(\frac{-7}{n}\right)$$

$$=\sum_{n\mid 3^{b-1}t}\left(\frac{-7}{n}\right)+\sum_{n\mid t}\left(\frac{-7}{3^b n}\right)$$

$$=\sum_{n\mid 3^{b-1}t}\left(\frac{-7}{n}\right)+\sum_{n\mid t}\left(\frac{-7}{3}\right)^b\left(\frac{-7}{n}\right)$$

$$=\sum_{n\mid 3^{b-1}t}\left(\frac{-7}{n}\right)-\sum_{n\mid t}\left(\frac{-7}{n}\right)$$

$$=\sum_{n\mid 3^{b-2}t}\left(\frac{-7}{n}\right)+\sum_{n\mid t}\left(\frac{-7}{3^{b-1}n}\right)-\sum_{n\mid t}\left(\frac{-7}{n}\right)$$

$$=\sum_{n\mid 3^{b-2}t}\left(\frac{-7}{n}\right)+\sum_{n\mid t}\left(\frac{-7}{3}\right)^{b-1}\left(\frac{-7}{n}\right)$$

$$-\sum_{n\mid t}\left(\frac{-7}{n}\right)=\sum_{n\mid 3^{b-2}t}\left(\frac{-7}{n}\right)+\sum_{n\mid t}\left(\frac{-7}{n}\right)$$

$$-\sum_{n\mid t}\left(\frac{-7}{n}\right)=\sum_{n\mid 3^{b-2}t}\left(\frac{-7}{n}\right)=e(3^{b-2}t)$$

且b是奇数，因此继续使用上法就会得到

$$e(3^{b}t)=e(3t)=\sum_{n\mid 3t}\left(\frac{-7}{n}\right)$$

$$=\sum_{n\mid t}\left(\frac{-7}{n}\right)+\sum_{n\mid t}\left(\frac{-7}{3n}\right)$$

$$=\sum_{n\mid t}\left(\frac{-7}{n}\right)+\sum_{n\mid t}\left(\frac{-7}{3}\right)\left(\frac{-7}{n}\right)$$

$$=\sum_{n\mid t}\left(\frac{-7}{n}\right)-\sum_{n\mid t}\left(\frac{-7}{n}\right)=0.$$

iii）最后证明若$3\nmid t$，则当b为偶数时，

$$e(3^{b}t)=e(t).$$

因为 $e(3^{b}t)=\sum_{n\mid 3^{b-1}t}\left(\frac{-7}{n}\right)+\sum_{n\mid t}\left(\frac{-7}{3^{b}n}\right)$

$$=\sum_{n\mid 3^{b-1}t}\left(\frac{-7}{n}\right)+\sum_{n\mid t}\left(\frac{-7}{n}\right)$$

$$=\sum_{n\mid 3^{b-2}t}\left(\frac{-7}{n}\right)+\sum_{n\mid t}\left(\frac{-7}{3^{b-1}n}\right)+\sum\left(\frac{-7}{n}\right)$$

$$=\sum_{n\mid 3^{b-2}t}\left(\frac{-7}{n}\right)-\sum_{n\mid t}\left(\frac{-7}{n}\right)+\sum_{n\mid t}\left(\frac{-7}{n}\right)$$

$$=\sum_{n\mid 3^{b-2}t}\left(\frac{-7}{n}\right)=e(3^{b-2}t)$$

且b为偶数，因此继续使用上法就一定可以得到$e(3^{b}t)=e(t)$。

习题8 若m为正奇数，则$m=x^2+7y^2$之解数为$2e(m)$；$2m=x^2+7y^2$之解数为0；$4k=x^2+7y^2$之解数为$2e(k)$，k为整数。

证：此时$d=-28$，$w=2$，且易证$h(-28)=1$。设$m=7^{s}m_1$，$s\geqslant 0$，$7\nmid m_1$。

(一) 先证$m=x^2+7y^2$的解数为$2e(m)$。当$s=0$时，$m=m_1$，$(m,d)=(m_1,-28)=1$，由定理10，此时解数为

$$\psi(m)=w\sum_{n\mid m}\left(\frac{d}{n}\right)=2\sum_{n\mid m}\left(\frac{-28}{n}\right)$$

$$=2\sum_{n\mid m}\left(\frac{-7}{n}\right)\left(\frac{2}{n}\right)^{2}=2\sum_{n\mid m}\left(\frac{-7}{n}\right)=2e(m)$$

当$s\geqslant 1$时，用归纳法予以证明．$s=1$时，$m=7m_1$，$l^2\equiv-28 \pmod 4$ 有解$l\equiv 0$，$2 \pmod 4$，其解数为2；$l^2\equiv-28 \pmod{7m_1}$ 的解数为$\prod_{p\mid 7m_1}\left(1+\left(\frac{-28}{p}\right)\right)=\prod_{p\mid 7m_1}\left(1+\left(\frac{-7}{p}\right)\right)$．故

$$l^2\equiv-28 \pmod{4\cdot 7m_1},\quad 0\leqslant l<2\cdot 7m_1$$

的解数为$\prod\limits_{p\mid 7m_1}\left(1+\left(\frac{-7}{p}\right)\right)$，$m=x^2+7y^2$的既约原解数为

$$w\prod_{p\mid 7m_1}\left(1+\left(\frac{-7}{p}\right)\right)=2\sum_{f\mid 7m_1}\left(\frac{-7}{f}\right)$$

其中f为正且无平方因子．故解数为

$$2\sum_{\substack{g^2\mid 7m_1\\ g>0}}\sum_{f\mid\frac{7m_1}{g^2}}\left(\frac{-7}{f}\right)=2\sum_{\substack{g^2\mid m_1\\ g>0}}\sum_{f\mid\frac{m_1}{g^2}}\left(\frac{-7}{f}\right)$$

$$+2\sum_{\substack{g^2\mid m_1\\ g>0}}\sum_{f\mid\frac{m_1}{g^2}}\left(\frac{-7}{7f}\right)$$

$$=2\sum_{\substack{g^2\mid m_1\\ g>0}}\sum_{f\mid\frac{m_1}{g^2}}\left(\frac{-7}{f}\right)=2\sum_{\substack{g^2\mid m_1\\ g>0}}\sum_{f\mid\frac{m_1}{g^2}}\left(\frac{-7}{fg^2}\right)$$

$$=2\sum_{n\mid m_1}\left(\frac{-7}{n}\right)=2\sum_{n\mid m}\left(\frac{-7}{n}\right)=2e(m)$$

此即$s=1$时结论成立．设$s=2$，…，t时，结论都成立，即

$$m=7^sm_1=x^2+7y^2,\quad 2\leqslant s\leqslant t$$

的解数为$2e(m)$．当$s=t+1$时，用与上面相同的方法可证其解数为

$$2\sum_{\substack{g^2\mid 7^{t+1}m_1\\ g>0}}\sum_{f\mid\frac{7^{t+1}m_1}{g^2}}\left(\frac{-7}{f}\right)$$

又因为 $$\sum_{\substack{g^2\mid 7^{t+1}m_1\\ g>0}}\sum_{f\mid\frac{7^{t+1}m_1}{g^2}}\left(\frac{-7}{f}\right)$$

$$=\sum_{\substack{g^2\mid 7m_1\\ g>0}}\sum_{f\mid\frac{7^tm_1}{g^2}}\left(\frac{-7}{f}\right)+\sum_{\substack{g^2\mid m_1\\ g>0}}\sum_{f\mid\frac{m_1}{g^2}}\left(\frac{-7}{7^{t+1}f}\right),$$

且
$$\sum_{\substack{g^2 \mid m_1 \\ g>0}} \sum_{f \mid \frac{m_1}{g^2}} \left(\frac{-7}{7^{t+1} f} \right) = 0$$

从而再由归纳假定
$$\sum_{\substack{g^2 \mid 7^t m_1 \\ g>0}} \sum_{f \mid \frac{7^t m_1}{g^2}} \left(\frac{-7}{f} \right) = e(m)$$

可立刻得到
$$m = 7^{t+1} m_1 = x^2 + 7y^2$$
的解数为 $2e(m)$。

（二）再证 $2m = x^2 + 7y^2$ 的解数为0．如果 $2m = x^2 + 7y^2$ 有解 x、y，显然它们同奇偶。但此两种情形均得出 $2 \equiv 0 \pmod 4$，故此种情形方程无解。

（三）k 为整数时，方程 $4k = x^2 + 7y^2$ 的解数为 $2e(k)$。设
$$4k = 2^r k_1,\quad r \geqslant 2,\quad 2 \nmid k_1$$

当 $r=2$ 时，$4k = 4k_1 = x^2 + 7y^2$。由于 k 为奇数，因此 x、y 必然同偶。因若同奇，就有 $4 \equiv 0 \pmod 8$，此不可能．设 $x = 2x_1$、$y = 2y_1$、$4k = x^2 + 7y^2$ 变为 $k = x_1^2 + 7y_1^2$．由本题前段所证，$k = x_1^2 + 7y_1^2$ 的解数为 $2e(k)$，从而 $4k = x^2 + 7y^2$ 的解数为 $2e(k)$，此即 $r=2$ 时结论成立．归纳假定
$$2^r k_1 = x^2 + 7y^2,\quad 3 \leqslant r \leqslant t$$
的解数为 $2e(k)$。当 $r = t+1$ 时，$4k = x^2 + 7y^2$ 写成 $2^{t+1} k_1 = x^2 + 7y^2$。$l^2 \equiv -28 \pmod 4$ 有解 $l \equiv 0,\ 2 \pmod 4$，其解数为2；$l^2 \equiv -28 \pmod{2^{t+1} k_1}$ 的解数为 $\prod_{p \mid 2^{t+1} k_1} \left(1 + \left(\frac{-28}{p} \right) \right) = \prod_{p \mid 2^{t+1} k_1} \left(1 + \left(\frac{-7}{p} \right) \right)$，从而

$l^2\equiv -28 \pmod{4\cdot 2^{t+1}k_1}$，$0\leqslant l<2\cdot 2^{t+1}k_1$ 的解数为 $\prod\limits_{p\mid 2^{t+1}k_1}\left(\left(1+\frac{-7}{p}\right)\right)$，$4k=x^2+7y^2$ 的既约原解数为

$$w\prod_{p\mid 2^{t+1}k_1}\left(1+\left(\frac{-7}{p}\right)\right)=2\sum_{f\mid 2^{t+1}k_1}\left(\frac{-7}{f}\right)$$

其中f为正且无平方因子。故$r=t+1$时，解数为

$$2\sum_{\substack{g^2\mid 2^{t+1}k_1\\ g>0}}\ \sum_{f\mid \frac{2^{t+1}k_1}{g^2}}\left(\frac{-7}{f}\right).$$

由归纳假定和$\left(\frac{-7}{2}\right)=1$有

$$\sum_{\substack{g^2\mid 2^{t}k_1\\ g>0}}\ \sum_{f\mid \frac{2^{t}k_1}{g^2}}\left(\frac{-7}{f}\right)=\sum_{\substack{g^2\mid 2^{t-1}k_1\\ g>0}}\ \sum_{f\mid \frac{2^{t-1}k_1}{g^2}}\left(\frac{-7}{f}\right)$$

$$+\sum_{\substack{g^2\mid k_1\\ g>0}}\ \sum_{f\mid \frac{k_1}{g^2}}\left(\frac{-7}{2^t f}\right)=e(k)+\sum_{\substack{g^2\mid k_1\\ g>0}}\ \sum_{f\mid \frac{k_1}{g^2}}\left(\frac{-7}{2}\right)^t\left(\frac{-7}{f}\right)$$

$$=e(k)+\sum_{\substack{g^2\mid k_1\\ g>0}}\ \sum_{f\mid \frac{k_1}{g^2}}\left(\frac{-7}{g^2 f}\right)=e(k)+\sum_{n\mid k_1}\left(\frac{-7}{n}\right)$$

$$=e(k)$$

因此 $\sum\limits_{n\mid k_1}\left(\frac{-7}{n}\right)=0$

$$\sum_{\substack{g^2 \mid 2^{t+1}k_1 \\ g>0}} \sum_{f \left| \frac{2^{t+1}k_1}{g^2} \right.} \left(\frac{-7}{f}\right) = \sum_{\substack{g^2 \mid 2^t k_1 \\ g>0}} \sum_{f \left| \frac{2^t k_1}{g^2} \right.} \left(\frac{-7}{f}\right)$$

$$+ \sum_{\substack{g^2 \mid k_1 \\ g>0}} \sum_{f \left| \frac{k_1}{g^2} \right.} \left(\frac{-7}{2^{t+1} f}\right) = e(k) + \sum_{\substack{g^2 \mid k_1 \\ g>0}} \sum_{f \left| \frac{k_1}{g^2} \right.} \left(\frac{-7}{g^2 f}\right)$$

$$= e(k) + \sum_{n \mid k_1} \left(\frac{-7}{n}\right) = e(k)$$

即 $4k = 2^{t+1}k_1 = x^2 + 7y^2$的解数为 $2e(k)$，结论对于$r = t+1$时也成立。

习题 9 若m为正奇数，则$x^2 + 7y^2 = 8m$恰有$e(m)$个正整数解。

证：设$k = 2m$，则 $4k = 8m$。由上题（三）可知 $4k = 8m = x^2 + 7y^2$的解数为

$$2e(k) = 2e(2m) = 2\sum_{n \mid 2m} \left(\frac{-7}{n}\right)$$

$$= 2\left(\sum_{n \mid m} \left(\frac{-7}{n}\right) + \sum_{n \mid m} \left(\frac{-7}{2n}\right)\right)$$

$$= 2\left(e(m) + \sum_{n \mid m} \left(\frac{-7}{2}\right)\left(\frac{-7}{n}\right)\right)$$

$$= 2\left(e(m) + \sum_{n \mid m} \left(\frac{-7}{n}\right)\right)$$

$$= 2(e(m) + e(m)) = 4e(m).$$

又由于x、y的符号包括x正y正、x正y负、x负y正、x负y负四种情形，所以

$$8m = x^2 + 7y^2$$

的正整数解数为$\frac{1}{4}(4e(m)) = e(m)$。

习题10　$0<m=x^2+xy+3y^2$之解数，等于m诸因子中$\equiv 1, 3, 4, 5, 9 \pmod{11}$者之个数减去$\equiv 2, 6, 7, 8, 10 \pmod{11}$者之个数所得之差的二倍。

证：此种情形$d=-11$，$w=2$，易证$h(-11)=1$。设$m=11^s m_1$，$s\geqslant 0$，$11\nmid m_1$。

i）当$s=0$时，方程为

$$m=m_1=x^2+xy+3y^2$$

且$(m, d)=(m_1, -11)=1$。由定理10，此方程解数为

$$w\sum_{n\mid m}\left(\frac{d}{n}\right)=2\sum_{n\mid m}\left(\frac{-11}{n}\right)$$

又因
$$\left(\frac{-11}{n}\right)=\begin{cases}\left(\frac{n}{11}\right),\text{当}(n, 11)=1\text{时}\\ 0,\quad\text{当}(n, 11)>1\text{时}\end{cases}$$

故
$$\left(\frac{-11}{n}\right)=\begin{cases}1,\quad\text{当}n\equiv 1, 3, 4, 5, 9 \pmod{11}\text{时}\\ 0,\quad\text{当}(n, 11)>1\text{时}\\ -1,\quad\text{当}n\equiv 2, 6, 7, 8, 10(\text{mod}11\text{时})\text{时}\end{cases}$$

所以$s=0$时，方程的解数为m的因子$\equiv 1, 3, 4, 5, 9 \pmod{11}$的个数减去$\equiv 2, 6, 7, 8, 10 \pmod{11}$的个数所得差的2倍。

ii）当$s\geqslant 1$时，下面用归纳法证明。$s=1$时，方程为$m=11m_1=x^2+xy+3y^2$。$l^2\equiv -11 \pmod 4$有解$l\equiv 1, 3 \pmod 4$，其解数为2；$l^2\equiv -11 \pmod{11m_1}$的解数为

$$\prod_{p\mid 11m_1}\left(1+\left(\frac{-11}{p}\right)\right)$$

从而　$l^2\equiv -11 \pmod{4\cdot 11m_1}$，$0\leqslant l<2\cdot 11m_1$

的解数为　$\prod_{p\mid 11m_1}\left(1+\left(\frac{-11}{p}\right)\right)$

$m=11m_1=x^2+xy+3y^2$的既约原解数为

$$2\prod_{p\mid 11m_1}\left(1+\left(\frac{-11}{p}\right)\right)=2\sum_{n\mid 11m}\left(\frac{-11}{f}\right)$$

其中f为正且无平方因子，因此方程$11m_1=x^2+xy+3y^2$的解数为：

$$2\sum_{\substack{g^2\mid 11m_1\\ g>0}}\sum_{f\mid\frac{11m_1}{g^2}}\left(\frac{-11}{f}\right)=2\Bigg(\sum_{\substack{g^2\mid m_1\\ g>0}}\sum_{f\mid\frac{m_1}{g^2}}\left(\frac{-11}{f}\right)$$

$$+\sum_{\substack{g^2\mid m_1\\ g>0}}\sum_{f\mid\frac{m_1}{g^2}}\left(\frac{-11}{11f}\right)\Bigg)=2\sum_{\substack{g^2\mid m_1\\ g>0}}\sum_{f\mid\frac{m_1}{g^2}}\left(\frac{-11}{f}\right)$$

$$=2\sum_{n\mid m_1}\left(\frac{-11}{n}\right)=2\sum_{n\mid m}\left(\frac{-11}{n}\right).$$

此即$s=1$时结论成立。设$s=t$、$t\geqslant 2$时结论成立，则$s=t+1$时，用相同方法可证

$$m=11^{t+1}m_1=x^2+xy+3y^2$$

的解数为
$$2\sum_{\substack{g^2\mid 11^{t+1}m_1\\ g>0}}\sum_{f\mid\frac{11^{t+1}m_1}{g^2}}\left(\frac{-11}{f}\right).$$

又因
$$\sum_{\substack{g^2\mid 11^{t+1}m_1\\ g>0}}\sum_{f\mid\frac{11^{t+1}m_1}{g^2}}\left(\frac{-11}{f}\right)=\sum_{\substack{g^2\mid 11^{t}m_1\\ g>0}}\sum_{f\mid\frac{11^{t}m_1}{g^2}}\left(\frac{-11}{f}\right)$$

$$+\sum_{\substack{g^2\mid m_1\\ g>0}}\sum_{f\mid\frac{m_1}{g^2}}\left(\frac{-11}{11^{t+1}f}\right)$$

且
$$\sum_{\substack{g^2\mid m_1\\ g>0}}\sum_{f\mid\frac{m_1}{g^2}}\left(\frac{-11}{11^{t+1}f}\right)=0$$

再由归纳假定 $\sum_{\substack{g^2 \mid 11^t m_1 \\ g>0}} \sum_{f \left| \frac{11^t m_1}{g^2} \right.} \left(\frac{-11}{f}\right) = \sum_{n \mid m} \left(\frac{-11}{n}\right)$

可得$m = 11^{t+1} m_1 = x^2 + xy + 3y^2$的解数为

$$2\sum_{n \mid m}\left(\frac{-11}{n}\right)$$

此即$s = t + 1$时结论仍然成立。综上所述，

$$0 < m = x^2 + xy + 3y^2$$

的解数等于m的因子$\equiv 1, 3, 4, 5, 9 \pmod{11}$的个数减去$\equiv 2, 6, 7, 8, 10 \pmod{11}$的个数的差的2倍。

§5 二次型的mod$q$相似

习题1 任何二个适合$\frac{d}{4} \equiv 2 \pmod 4$的二次型必mod 4相似。

证： 设$\{a, b, c\}$，$\{a_1, b_1, c_1\}$是合条件

$$\frac{d}{4} \equiv \frac{d_1}{4} \equiv 2 \pmod 4$$

的两个二次型．d、d_1分别是它们的判别式．因为$2 \mid d$，$2 \mid d_1$，故$2 \mid b$，$2 \mid b_1$．又因为

$$\frac{d}{4} = \left(\frac{b}{2}\right)^2 - ac,\ \frac{d_1}{4} = \left(\frac{b_1}{2}\right)^2 - a_1c_1$$

所以可将证明分为下列几种情形：

（一）当$b \equiv 0 \pmod 4$，$b_1 \equiv 0 \pmod 4$时．不妨设$b = b_1 = 0$，从而只需证明

$$\{a,\ 0,\ c\} \sim \{a_1,\ 0,\ c_1\} \pmod 4$$

即可。由

$$\frac{d}{4} \equiv -ac \equiv 2 \pmod 4,\quad ac \equiv 2 \pmod 4$$

有

$$\begin{cases} a \equiv 1 \pmod 4 \\ c \equiv 2 \pmod 4 \end{cases} \qquad 〈Ⅰ〉$$

或

$$\begin{cases} a \equiv 2 \pmod 4 \\ c \equiv 1 \pmod 4 \end{cases} \qquad 〈Ⅱ〉$$

从〈Ⅰ〉得$ax^2 + cy^2 \equiv x^2 + 2y^2 \pmod 4$，即

$$\{a,\ 0,\ c\} \sim \{1,\ 0,\ 2\} \pmod 4.$$

从〈Ⅱ〉得$ax^2 + cy^2 \equiv 2x^2 + y^2 \pmod 4$．设

$$x = rX + sY = Y,\quad y = tX + uY = X$$

则

$$ax^2 + cy^2 \equiv X^2 + 2Y^2 \pmod 4$$

又因为$(ru - st,\ 4) = (-1,\ 4) = 1$，故

$$\{a,\ 0,\ c\} \sim \{1,\ 0,\ 2\} \pmod 4$$

同理可证 $\{a_1,\ 0,\ c_1\} \sim \{1,\ 0,\ 2\} \pmod 4$

所以 $\{a,\ 0,\ c\} \sim \{a_1,\ 0,\ c_1\} \pmod 4$．

（二）当$b \equiv 0 \pmod 4$、$b_1 \equiv 2 \pmod 4$时．由（一），只需证明

$$\{a_1,\ b_1,\ c_1\} \sim \{1,\ 0,\ 2\} \pmod 4$$

即可．因为$b_1 \equiv 2 \pmod 4$，因此

$$\frac{d_1}{4} = \left(\frac{b_1}{2}\right)^2 - a_1c_1 \equiv 2 \pmod 4$$

给出$a_1c_1 \equiv 3 \pmod 4$，从而有

$$\begin{cases} a_1 \equiv 3 \pmod 4 \\ c_1 \equiv 1 \pmod 4 \end{cases} \qquad 〈Ⅲ〉$$

或 $$\begin{cases} a_1 \equiv 1 \pmod 4 \\ c_1 \equiv 3 \pmod 4 \end{cases} \qquad \langle \text{IV} \rangle$$

不妨设〈 I 〉成立。命

$$x = 2X + Y,\quad y = X + Y$$

则

$$a_1x^2 + b_1xy + c_1y^2 \equiv 3x^2 + 2xy + y^2$$
$$\equiv 3(2X+Y)^2 + 2(2X+Y)(X+Y)^2 + (X+Y)^2$$
$$\equiv X^2 + 2Y^2 \pmod 4;$$

又因为 $(ru-st,\ 4) = (1,\ 4) = 1$，故

$$\{a_1,\ b_1,\ c_1\} \sim \{1,\ 0,\ 2\} \pmod 4.$$

（三）当 $b \equiv 2 \pmod 4$，$b_1 \equiv 0 \pmod 4$ 时，可化为（二）证明。

（四）当 $b \equiv 2 \pmod 4$，$b_1 \equiv 2 \pmod 4$ 时．由（二）可得

$$\{a,\ b,\ c\} \sim \{1,\ 0,\ 2\} \pmod 4$$
$$\{a_1,\ b_1,\ c_1\} \sim \{1,\ 0,\ 2\} \pmod 4$$

从而有

$$\{a,\ b,\ c\} \sim \{a_1,\ b_1,\ c_1\} \pmod 4.$$

由（一）～（四）可知，当 $\frac{d}{4} \equiv \frac{d_1}{4} \equiv 2 \pmod 4$ 时，

$$\{a,\ b,\ c\} \sim \{a_1,\ b_1,\ c_1\} \pmod 4.$$

习题2 任何二个适合 $\frac{d}{4} \equiv 1 \pmod 4$ 的二次型必 mod 4 相似，但此两个二次型 $\{a,\ b,\ c\}$，$\{a_1,\ b_1,\ c_1\}$ 必须满足条件

$$(a,\ b,\ c) = (a_1,\ b_1,\ c_1) = 1.$$

证： 同习题 1 一样，可将证明分为如下四种情形。

（一）当$b\equiv 0\pmod 4$，$b_1\equiv 0\pmod 4$时．不妨设$b=b_1=0$，因此只需证明

$$\{a,\ 0,\ c\}\sim\{a_1,\ 0,\ c_1\}\pmod 4$$

即可．由

$$\frac{d}{4}\equiv -ac\equiv 1\pmod 4,\quad ac\equiv 3\pmod 4$$

有
$$\begin{cases}a\equiv 1\pmod 4\\ c\equiv 3\pmod 4\end{cases}\qquad\langle\,\mathrm{I}\,\rangle$$

或
$$\begin{cases}a\equiv 3\pmod 4\\ c\equiv 1\pmod 4\end{cases}\qquad\langle\,\mathrm{II}\,\rangle$$

由〈Ⅰ〉有$ax^2+cy^2\equiv x^2+3y^2\pmod 4$，即

$$\{a,\ 0,\ c\}\sim\{1,\ 0,\ 3\}\pmod 4.$$

由〈Ⅱ〉有$ax^2+cy^2\equiv 3x^2+y^2\pmod 4$．

设　$x=rX+sY=Y$，$y=tX+uY=X$，

则　$ax^2+cy^2\equiv X^2+3Y^2\pmod 4$．

又因为$(ru-st,\ 4)=1$，故有

$$\{a,\ 0,\ c\}\sim\{1,\ 0,\ 3\}\pmod 4$$

同理可证　$\{a_1,\ 0,\ c_1\}\sim\{1,\ 0,\ 3\}\pmod 4$

故　$\{a,\ 0,\ c\}\sim\{a_1,\ 0,\ c_1\}\pmod 4$

（二）当$b\equiv 0\pmod 4$，$b_1\equiv 2\pmod 4$时．由（一）可知，只需证明

$$\{a_1,\ b_1,\ c_1\}\sim\{1,\ 0,\ 3\}\pmod 4$$

即可．

由　$\dfrac{d_1}{4}\equiv\left(\dfrac{b_1}{2}\right)^2-a_1c_1\equiv 1\pmod 4$

且 $(a_1, b_1, c_1)=1$ 有

$$\begin{cases} a_1\equiv 0 \pmod 4 \\ c_1\equiv 1 \pmod 4 \end{cases} \qquad \langle \text{I} \rangle$$

或

$$\begin{cases} a_1\equiv 0 \pmod 4 \\ c_1\equiv 3 \pmod 4 \end{cases} \qquad \langle \text{II} \rangle$$

或

$$\begin{cases} a_1\equiv 1 \pmod 4 \\ c_1\equiv 0 \pmod 4 \end{cases} \qquad \langle \text{III} \rangle$$

或

$$\begin{cases} a_1\equiv 3 \pmod 4 \\ c_1\equiv 0 \pmod 4 \end{cases} \qquad \langle \text{IV} \rangle$$

对于〈 Ⅰ 〉，命 $x=2X+Y,\ y=X+Y$

则 $a_1x^2+b_1xy+c_1y^2\equiv 2xy+y^2$

$\equiv 2(2X+Y)(X+Y)+(X+Y)^2$

$\equiv X^2+3Y^2 \pmod 4$

此即 $\{a_1, b_1, c_1\}\sim\{1, 0, 3\} \pmod 4$

对于〈 Ⅱ 〉，命 $x=X+2Y,\ y=X+Y$

则

$$a_1x^2+b_1xy+c_1y^2\equiv 2xy+3y^2$$

$$\equiv 2(X+2Y)(X+Y)+3(X+Y)^2$$

$$\equiv X^2+3Y^2 \pmod 4$$

此即 $\{a_1, b_1, c_1\}\sim\{1, 0, 3\} \pmod 4$

对于〈 Ⅲ 〉，可化为〈 Ⅰ 〉证明。

对于〈 Ⅳ 〉，可化为〈 Ⅱ 〉证明。因此，当 $b\equiv 0 \pmod 4$，$b_1\equiv 2 \pmod 4$ 时，总有

$$\{a, b, c\}\sim\{a_1, b_1, c_1\} \pmod 4.$$

（三）当 $b\equiv 2 \pmod 4$，$b_1\equiv 0 \pmod 4$ 时，可化为（二）证明。

（四）当$b\equiv 2 \pmod 4$，$b_1\equiv 2 \pmod 4$时，由（二）有

$$\{a, b, c\} \sim \{1, 0, 3\} \pmod 4$$

$$\{a_1, b_1, c_1\} \sim \{1, 0, 3\} \pmod 4$$

故有 $$\{a, b, c\} \sim \{a_1, b_1, c_1\} \pmod 4.$$

由（一）～（四）可知，当$\frac{d}{4}\equiv\frac{d_1}{4}\equiv 1 \pmod 4$，且$(a, b, c)=(a_1, b_1, c_1)=1$时，

$$\{a, b, c\} \sim \{a_1, b_1, c_1\} \pmod 4.$$

说明： 如果不添加

$$(a, b, c)=(a_1, b_1, c_1)=1$$

这个限制，就不一定有

$$\{a, b, c\} \sim \{a_1, b_1, c_1\} \pmod 4.$$

例如：取a_1、b_1、c_1合条件

$$a_1\equiv 0,\ b_1\equiv 2,\ c_1\equiv 2 \pmod 4$$

它们显然满足 $\frac{d_1}{4}\equiv\left(\frac{b_1}{2}\right)^2-a_1c_1\equiv 1 \pmod 4$，

但是 $$\{a_1, b_1, c_1\} \sim \{1, 0, 3\} \pmod 4$$

不能成立，否则，一定可以找到整数r、s、t、u，使得

$$\begin{aligned} &a_1x^2+b_1xy+c_1y^2\equiv 2xy+2y^2\\ &\equiv 2(rX+sY)(tX+uY)+2(tX+uY)^2\\ &\equiv(2rt+2t^2)X^2+(2ru+2st+4tu)XY\\ &+(2su+2u^2)Y^2\\ &\equiv X^2+3Y^2 \pmod 4 \end{aligned}$$

即有

$$\begin{cases} 2rt+2t^2\equiv 1 \pmod 4 & (1)\\ 2ru+2st+4tu\equiv 0 \pmod 4 & (2)\\ 2su+2u^2\equiv 3 \pmod 4 & (3) \end{cases}$$

但是（1）、（3）显然不成立。因此原题不添加条件

$$(a, b, c)=(a_1, b_1, c_1)=1$$

可能有误.

习题 3 任何适合$\frac{d}{4}\equiv 1 \pmod 4$的型必与

$$x^2+3y^2, \quad x^2+7y^2$$

之一mod 8相似，且仅与其中之一mod 8相似. 并由此推出任何二个具有相同判别式d，而$\frac{d}{4}\equiv 1 \pmod 4$的二次型，必为mod 8相似，但所讨论的二次型必须合条件：系数的最大公因数为1。

证：不失一般，只考虑形如$\{a, 0, c\}$的二次型即可. 由

$\frac{d}{4}\equiv -ac\equiv 1 \pmod 4$，$ac\equiv 3 \pmod 4$

有
$$\begin{cases} a\equiv 1 \pmod 4 \\ c\equiv 3 \pmod 4 \end{cases} \qquad \langle \text{I} \rangle$$

或
$$\begin{cases} a\equiv 3 \pmod 4 \\ c\equiv 1 \pmod 4 \end{cases} \qquad \langle \text{II} \rangle$$

不失一般，假设〈I〉成立，则

$$a\equiv 1 \pmod 4$$

给出
$$a\equiv 1, \ 5 \pmod 8;$$

$$c\equiv 3 \pmod 4$$

给出
$$c\equiv 3, \ 7 \pmod 8.$$

i）当$a\equiv 1 \pmod 8$，$c\equiv 3 \pmod 8$时，

$$ax^2+cy^2\equiv x^2+3y^2 \pmod 8$$

此即 $\{a, 0, c\}\sim\{1, 0, 3\} \pmod 8$.

ii）当$a\equiv 1 \pmod 8$，$c\equiv 7 \pmod 8$时，

$$ax^2+cy^2\equiv x^2+7y^2 \pmod 8,$$

此即 $\{a, 0, c\} \sim \{1, 0, 7\} \pmod 8$.

iii) 当$a \equiv 5 \pmod 8$，$c \equiv 3 \pmod 8$时，

设 $x = rX + sY = X + 2Y$，$y = tX + uY = 2X + Y$，

则 $ax^2 + cy^2 \equiv 5x^2 + 3y^2 \equiv 5(X + 2Y)^2 + 3(2X + Y)^2 \equiv X^2 + 7Y^2 \pmod 8$，

又因为 $(ru - st, 8) = 1$，故

$$\{a, 0, c\} \sim \{1, 0, 7\} \pmod 8.$$

Ⅳ) 当$a \equiv 5 \pmod 8$，$c \equiv 7 \pmod 8$时。

仍然设 $x = X + 2Y$，$y = 2X + Y$，

则 $ax^2 + cy^2 \equiv 5x^2 + 7y^2 \equiv 5(X + 2Y)^2 + 7(2X + Y)^2 \equiv X^2 + 3Y^2 \pmod 8$

此即 $\{a, 0, c\} \sim \{1, 0, 3\} \pmod 8$

由i)～Ⅳ)可知，二次型 $\{a, 0, c\}$ 如果合条件$\frac{d}{4} \equiv 1 \pmod 4$，

那么它就一定与

$$x^2 + 3y^2,\quad x^2 + 7y^2$$

之一mod 8相似；而要证它仅与其中之一mod 8相似，只需证明$x^2 + 3y^2$与$x^2 + 7y^2$不mod 8相似就可以了。

下面使用反证法。如果

$$\{1, 0, 3\} \sim \{1, 0, 7\} \pmod 8$$

则一定有一整系数变换

$$x = rX + sY,\quad y = tX + uY$$

合条件 $(ru - st, 8) = 1$

使得 $x^2 + 3y^2 \equiv X^2 + 7Y^2 \pmod 8$

成立。即

$$\begin{aligned} x^2 + 3y^2 &\equiv (rX + sY)^2 + 3(tX + uY)^2 \\ &\equiv (r^2 + 3t^2)X^2 + (2rs + 6tu)XY + (s^2 + 3u^2)Y^2 \\ &\equiv X^2 + 7Y^2 \pmod 8, \end{aligned}$$

从而有

$$\begin{cases} r^2+3t^2\equiv 1 \pmod 8 & (1)\\ rs+3tu\equiv 0 \pmod 4 & (2)\\ s^2+3u^2\equiv 7 \pmod 8 & (3)\end{cases}$$

由（1）知r、t一奇一偶．当r奇t偶时，有$4|t$．由（2），$4|s$；由（3），$3u^2\equiv 7\pmod 8$，此不可能．而当r偶t奇时，设$r=2m$，（1）给出

$4m^2+3\equiv 1\pmod 8$，$2m^2+1\equiv 0\pmod 4$，此也不可能．所以，x^2+3y^2与x^2+7y^2不能mod 8相似．

下面再证明任何两个具有相同判别式d，而$\frac{d}{4}\equiv 1\pmod 4$的二次型必为mod 8相似．设$\{a, 0, c\}$、$\{a_1, 0, c_1\}$为具有相同判别式$d$且$\frac{d}{4}\equiv 1\pmod 4$的两个二次型．不失一般，只需证明，如果

$$ax^2+cy^2\equiv X^2+3Y^2\pmod 8$$

就有
$$a_1x^2+c_1y^2\equiv X^2+3Y^2\pmod 8$$

即可．由上面讨论知道，

$$ax^2+cy^2\equiv X^2+3Y^2\pmod 8$$

给出　$a\equiv 1$，$c\equiv 3\pmod 8$

或者　$a\equiv 5$，$c\equiv 7\pmod 8$

不妨设$a\equiv 1$，$c\equiv 3\pmod 8$．如果

$$a_1x^2+c_1y^2\equiv X^2+7Y^2\pmod 8$$

则一定有　$a_1\equiv 1$，$c_1\equiv 7\pmod 8$

或者　$a_1\equiv 5$，$c_1\equiv 3\pmod 8$．

i) 当$a_1\equiv 1$，$c_1\equiv 7\pmod 8$时

$$a_1x^2+c_1y^2\equiv X^2+7Y^2\pmod 8,$$

$$a_1c_1x^2+c_1{}^2y^2\equiv c_1X^2+7c_1Y^2\pmod 8$$

又因为$\frac{d}{4}=ac=a_1c_1$，故有

$$acx^2+y^2\equiv 7X^2+Y^2 \pmod 8$$

$$ac^2x^2+cy^2\equiv 7cX^2+cY^2 \pmod 8$$

$$ax^2+cy^2\equiv 5X^2+3Y^2 \pmod 8$$

此即 $\{a, 0, c\}\sim\{5, 0, 3\} \pmod 8$

又由习题前半部分证明知道

$$\{5, 0, 3\}\sim\{1, 0, 7\} \pmod 8$$

故 $\{a, 0, c\}\sim\{1, 0, 7\} \pmod 8$

此与 $\{a, 0, c\}\sim\{1, 0, 3\} \pmod 8$ 矛盾。

ii) 当$a_1\equiv 5$，$c_1\equiv 3 \pmod 8$ 时：

$$a_1x^2+c_1y^2\equiv X^2+7Y^2 \pmod 8$$

$$a_1c_1x^2+c_1{}^2y^2\equiv c_1X^2+7c_1Y^2 \pmod 8$$

$$acx^2+y^2\equiv 3X^2+5Y^2 \pmod 8$$

$$ac^2x^2+cy^2\equiv 3cX^2+5cY^2 \pmod 8$$

$$ax^2+cy^2\equiv X^2+7Y^2 \pmod 8$$

此即 $\{a, 0, c\}\sim\{1, 0, 7\} \pmod 8$

也与 $\{a, 0, c\}\sim\{1, 0, 3\} \pmod 8$ 相矛盾。

由i)、ii)便知，如果 $\{a, 0, c\}\sim\{1, 0, 3\} \pmod 8$，则一定有

$$\{a_1, 0, c_1\}\sim\{1, 0, 3\} \pmod 8.$$

此即 $\{a, 0, c\}\sim\{a_1, 0, c_1\} \pmod 8$.

说明： 原题没有二次型的系数互素这个条件，可能有误，理由与习题2的说明相同。

习题4 命q为任一正整数．任二个二次型对mod$q$相似之必要且充分条件为其特征系全同．

此题是错误的。现说明如下：设两个二次型 $\{a, b, c\}$、$\{a_1, b_1, c_1\}$ 的判别式分别为d和d_1，dd_1非平方数，并且它们

的特征系完全相同。我们可任取一素数p，使得

$$\left(\frac{d}{p}\right) \neq \left(\frac{d_1}{p}\right)$$

如果本题结论正确，那么对任意正整数q，都有

$$\{a, b, c\} \sim \{a_1, b_1, c_1\} \pmod{q}$$

当然，$q=p$时也应该有

$$\{a, b, c\} \sim \{a_1, b_1, c_1\} \pmod{p}$$

因此必存在一个整系数变换

$$x = rX + sY,\quad y = tX + uY,$$
$$(ru - st,\ p) = 1 \tag{1}$$

使 $ax^2 + bxy + cy^2 \equiv a_1X^2 + b_1XY + c_1Y^2 \pmod{p}$

从而 $d_1 \equiv (ru - st)^2 d \pmod{p}$

故

$$\left(\frac{d_1}{p}\right) = \left(\frac{d}{p}\right)$$

此与$\left(\frac{d}{p}\right) \neq \left(\frac{d_1}{p}\right)$相矛盾。

请看下面三个例子。

例1 二次型$x^2 + xy + y^2$的判别式为$d = -3$，特征系为$\left(\frac{1}{3}\right) = 1$；二次型$x^2 - 3xy$的判别式为$d_1 = 9$，特征系为$\left(\frac{1}{3}\right) = 1$。该两个二次型的特征系全同，取$q = 11$。由本题的结论，定有整系数变换(1)，使得

$$x^2 + xy + y^2 \equiv X^2 - 3XY \pmod{11}$$

从而有 $d_1 \equiv (ru - st)^2 d \pmod{11}$.

故

$$\left(\frac{d_1}{11}\right) = \left(\frac{d}{11}\right)$$

即
$$1=\left(\frac{9}{11}\right)=\left(\frac{-3}{11}\right)=-1$$

此不可能。

例 2　二次型$x^2+3xy+y^2$的判别式为$d=5$，特征系为$\left(\frac{1}{5}\right)=1$；二次型$x^2+5xy$的判别式为$d_1=5^2$，特征系为$\left(\frac{1}{5}\right)=1$. 该两个二次型的特征系全同，取$q=3$. 如果本题结论成立，同例1一样可得
$$1=\left(\frac{5^2}{3}\right)=\left(\frac{5}{3}\right)=-1$$

此也不可能。

例 3　二次型x^2+8y^2的判别式为$d=-2^5$,特征系为$\delta(1)=\varepsilon(1)=\delta(1)\varepsilon(1)=1$；二次型$x^2+16y^2$的判别式为$d_1=-2^6$，特征系为$\delta(1)=\varepsilon(1)=\delta(1)\varepsilon(1)=1$. 该两个二次型的特征系全同，取$q=3$. 如果本题结论成立，同例1可得
$$-1=\left(\frac{2}{3}\right)=\left(\frac{-2^6}{3}\right)=\left(\frac{-2^5}{3}\right)=\left(\frac{1}{3}\right)=1$$

此仍然不可能。

在这三个反例中，两个二次型的判别式的符号分别属于异号、同正、同负三种情形。

§6　二次型的特征系　族

习题　如例题，研究$d=-20$，-24，-32，-35，-51，-75时之情况。

解：（一）　当$d=-20$时,有两个正定已化原型$\{1, 0, 5\}$，$\{2, 2, 3\}$. 取$k=1, 7$（$1=1\cdot1^2+0\cdot1\cdot0+5\cdot0^2$；

$7=2\cdot1^2+2\cdot1\cdot1+3\cdot1^2$）．由于$d=-2^2\times5$，所以此二型的特征系由下表给出：

型	$\left(\frac{k}{5}\right)$	$\delta(k)$
{1，0，5}	1	1
{2，2，3}	−1	−1

此表完全说明每族包有一类，由此得出$k\equiv1$，7（mod10）时，$\psi(k)$各表第一、第二型的解数．更具体些说，当$k\equiv1$（mod10）时，$x^2+5y^2=k$的解数为

$$\psi(k)=2\sum_{n\mid k}\left(\frac{-20}{n}\right)$$

当$k\equiv7$（mod10）时，方程$x^2+5y^2=k$无解。

（二）当$d=-24$时，有两个正定已化原型{1，0，6}，{2，0，3}．取$k=1$，5（$1=1\cdot1^2+6\cdot0^2$；$5=2\cdot1^2+3\cdot1^2$）．由于$d=-2^3\times3$，故此二型的特征系由下表给出：

型	$\left(\frac{k}{3}\right)$	$\delta(k)$
{1，0，6}	1	1
{2，0，3}	−1	−1

此表完全说明每族包有一类．由此得出，当$k\equiv1,5$(mod6)时，$\psi(k)$各表第一、第二型的解数．更具体些说，当$k\equiv1$（mod6）时，

$$\psi(k)=2\sum_{n\mid k}\left(\frac{-24}{n}\right)$$

表$k=x^2+6y^2$的解数，当$k\equiv5$（mod6）时，方程$k=x^2+6y^2$无

解.

（三）当$d=-32$时，有两个正定已化原型｛1，0，8｝，｛3，2，3｝.取$k=1,3$（$1=1\cdot1^2+8\cdot0^2$；$3=3\cdot1^2+2\cdot1\cdot0+3\cdot0^2$）．由于$d=-2^5$，故此二型的特征系由下表给出：

型	$\delta(k)$	$\varepsilon(k)$	$\delta(k)\ \varepsilon(k)$
{1，0，8}	1	1	1
{3，2，3}	－1	－1	1

此表完全说明每族包有一类．由此得出，$k\equiv1,3\pmod 8$时，$\psi(k)$各表第一、第二型的解数．当$k\equiv1$ (mod) 时，方程$k=x^2+8y^2$的解数为

$$\psi(k)=2\sum_{n\mid k}\left(\frac{-32}{n}\right)$$

当$k\equiv3\pmod 8$时，$k=x^2+8y^2$无解.

（四）当$d=-35$时，有两个正定已化原型｛1，1，9｝，｛3，1，3｝．取$k=11$，17（$11=1^2+1\cdot1+9\cdot1^2$；$17=3\cdot1^2+1\cdot2+3\cdot2^2$）．由于$d=-5\times7$，故此二型的特征系由下表给出：

型	$\left(\frac{k}{5}\right)$	$\left(\frac{k}{7}\right)$
{1，1，9}	1	1
{3，1，3}	－1	－1

$\left(\frac{k}{5}\right)=\left(\frac{k}{7}\right)=1$给出

$$k\equiv1,\ 4,\ 9,\ 11,\ 16,\ 29\pmod{35};$$

$\left(\frac{k}{5}\right)=\left(\frac{k}{7}\right)=-1$ 给出

$$k\equiv 3,\ 12,\ 13,\ 17,\ 27,\ 33 \pmod{35}.$$

即如果

$k\equiv 2,\ 6,\ 8,\ 18,\ 19,\ 22,\ 23,\ 26,\ 31,\ 32, 34 \pmod{35}$ 时，

方程

$$k=x^2+xy+9y^2$$

与

$$k=3x^2+xy+3y^2$$

都无解。而当$k\equiv 1,\ 4,\ 9,\ 11,\ 16,\ 29 \pmod{35}$时，方程$x^2+xy+9y^2=k$的解数为

$$\psi(k)=2\sum_{n\mid k}\left(\frac{-35}{n}\right);$$

而当$k\equiv 3,\ 12,\ 13,\ 17,\ 27,\ 33 \pmod{35}$ 时，方程$3x^2+xy+3y^2=k$的解数也是

$$\psi(k)=2\sum_{n\mid k}\left(\frac{-35}{n}\right).$$

（五）当$d=-51$时，有两个正定已化原型 $\{1,1,13\}$，$\{3,3,5\}$。取$k=1, 11$（$1=1^2+1\cdot 0+13\cdot 0^2$；$11=3\cdot 1^2+3\cdot 1\cdot 1+5\cdot 1^2$）。由于$d=-3\times 17$，故此二型的特征系由下表给出：

型	$\left(\frac{k}{3}\right)$	$\left(\frac{k}{17}\right)$
$\{1, 1, 13\}$	1	1
$\{3, 3, 5\}$	-1	-1

$\left(\frac{k}{3}\right)=\left(\frac{k}{17}\right)=1$ 给出

$$k\equiv 1,\ 4,\ 13,\ 16,\ 19,\ 25,\ 43,\ 49 \pmod{51};$$

$\left(\frac{k}{3}\right)=\left(\frac{k}{17}\right)=-1$ 给出

$k\equiv 5, 11, 14, 20, 23, 29, 44 \pmod{51}$。即如果$k\equiv = 2, 7, 8, 10, 22, 26, 28, 31, 32, 35, 37, 38, 40, 41, 46, 47, 50 \pmod{51}$ 时，k不能被此二型中任何一个表出。而当$k\equiv 1, 4, 13, 16, 19, 25, 43, 49 \pmod{51}$ 时，$k=x^2+xy+13y^2$的解数为

$$\psi(k)=2\sum_{n\mid k}\left(\frac{-51}{n}\right).$$

当$k\equiv 5, 11, 14, 20, 23, 29, 44 \pmod{51}$ 时，$k=3x^2+3xy+5y^2$的解数也是

$$\psi(k)=2\sum_{n\mid k}\left(\frac{-51}{n}\right).$$

（六）当$d=-75$时，有两个正定已化原型 $\{1, 1, 19\}$，$\{3, 3, 7\}$。取$k=1, 13$（$1=1^2+1\cdot 0+19\cdot 0^2$; $13=3\cdot 1^2+3\cdot 1\cdot 1+7\cdot 1^2$）。由于$d=-3\times 5^2$，故此二型的特征系由下表给出：

型	$\left(\frac{k}{3}\right)$	$\left(\frac{k}{5}\right)$
$\{1, 1, 19\}$	1	1
$\{3, 3, 7\}$	1	-1

$\left(\frac{k}{3}\right)=\left(\frac{k}{5}\right)=1$ 给出

$$k\equiv 1, 4 \pmod{15};$$

$\left(\frac{k}{3}\right)=1$，$\left(\frac{k}{5}\right)=1$ 给出

$$k\equiv 7, 13 \pmod{15}.$$

即如果$k\equiv 2$，8，11，14(mod15) 时，k不能用此二型中任何一个表出。当$k\equiv 1$，4 (mod15) 时，方程 $k=x^2+xy+19y^2$ 的解数为

$$\psi(k)=2\sum_{n\mid k}\left(\frac{-75}{n}\right);$$

当$k\equiv 7$，13 (mod15) 时，方程$k=3x^2+3xy+7y^2$的解数也是

$$\psi(k)=2\sum_{n\mid k}\left(\frac{-75}{n}\right).$$

§11 基本判别式

习题 试证若d为基本判别式，则$\left(\frac{d}{n}\right)$为一模$|d|$的实原特征。

证：若d为基本判别式，由定义可知d为下列三种情形之一：

1) d不含奇素数平方因子且d为奇数。

2) d不含奇素数平方因子，并且

$$d=16t+12=2^2(4t+3).$$

3) d不含奇素数平方因子，并且

$$d=16t+8=2^3(2t+1).$$

由12.3定理1：

对于1)，
$$\left(\frac{d}{n}\right)=\left(\frac{n}{|d|}\right).$$

对于2)，
$$\left(\frac{d}{n}\right)=\left(\frac{2}{n}\right)^2(-1)^{\frac{4t+3-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{|4t+3|}\right)$$

$$=(-1)^{\frac{n-1}{2}}\left(\frac{n}{|d|/4}\right).$$

对于3)，
$$\left(\frac{d}{n}\right)=\left(\frac{2}{n}\right)^{3}(-1)^{\frac{2t+1-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{|2t+1|}\right)$$

$$=\left(\frac{2}{n}\right)(-1)^{\frac{t(n-1)}{2}}\left(\frac{n}{|d|/8}\right).$$

因为当 $(n,\ d)=1$ 时，可推出 $2\mid n-1$，故

$$\left(\frac{d}{n}\right)=\begin{cases}(-1)^{\frac{n^2-1}{8}}\left(\frac{n}{|d|/8}\right), & \text{当} 2\mid t \text{时},\\ (-1)^{\frac{n^2-1}{8}+\frac{n-1}{2}}\left(\frac{n}{|d|/8}\right), & \text{当} 2\nmid t \text{时}.\end{cases}$$

再由7.3 可 知$\left(\frac{d}{n}\right)$为模$|d|$的实原特征。

§12 类数公式

习题 1 试用上二定理中所用之方法，以直接证明

$$|d|\sum_{r=1}^{[\frac{1}{2}|d|]}\left(\frac{d}{r}\right)=\left(\left(\frac{d}{2}\right)-2\right)\sum_{r=1}^{|d|}\left(\frac{d}{r}\right)r.$$

证： i) 当$d<$时，完全照12.12.4的证明方法可以得到

$$\pi\sum_{r=1}^{[\frac{1}{2}|d|]}\left(\frac{d}{r}\right)=\sqrt{|d|}\left(2-\left(\frac{d}{2}\right)\right)K(d)$$

因此
$$|d|\sum_{r=1}^{[\frac{1}{2}|d|]}\left(\frac{d}{r}\right)=\left(2-\left(\frac{d}{2}\right)\right)\frac{|d|^{\frac{3}{2}}}{\pi}K(d) \qquad (1)$$

又因为12.12.2 给出 $K(d)=-\frac{\pi}{|d|^{3/2}}\sum_{r=1}^{|d|}\left(\frac{d}{r}\right)r$ （2）

把（2）代入（1）就有

$$|d|\sum_{r=1}^{[\frac{1}{2}|d|]}\left(\frac{d}{r}\right)=\left(\left(\frac{d}{2}\right)-2\right)\sum_{r=1}^{|d|}\left(\frac{d}{r}\right)r.$$

ii） 当$d>0$时。如12.12.2的证明可得

$$\sqrt{d}\,K(d)\left(\frac{d}{2}\right)=\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{d}{2n}\right)\sqrt{d}=\sum_{n=1}^{\infty}\frac{1}{n}\sum_{r=1}^{d-1}\left(\frac{d}{r}\right)e^{\frac{4n\pi ri}{d}}$$

比较上式虚部得

$$0=\sum_{n=1}^{\infty}\frac{1}{n}\sum_{r=1}^{d-1}\left(\frac{d}{r}\right)\sin\frac{4n\pi r}{d}=\sum_{r=1}^{d-1}\left(\frac{d}{r}\right)\sum_{n=1}^{\infty}\frac{1}{n}\sin\frac{4n\pi r}{d}$$

$$=\sum_{1\leqslant r\leqslant\frac{1}{2}d}\left(\frac{d}{r}\right)\left(\left(\frac{\pi}{2}\right)-\frac{2\pi r}{d}\right)$$

$$+\sum_{\frac{1}{2}d<r\leqslant d-1}\left(\frac{d}{r}\right)\left(\frac{\pi}{2}-\frac{2\pi r}{d}+\pi\right)$$

注意到$\sum_{r=1}^{d-1}\left(\frac{d}{r}\right)=0$，从而上式给出

$$\sum_{r=1}^{d-1}\left(\frac{d}{r}\right)r=\frac{d}{2}\sum_{\frac{1}{2}d<r\leqslant d-1}\left(\frac{d}{r}\right) \qquad （3）$$

由12.3.3得 $\left(\frac{d}{r}\right)=\left(\frac{d}{d-r}\right)$

所以 $$\sum_{1\leqslant r\leqslant\frac{1}{2}d}\left(\frac{d}{r}\right)=\sum_{1\leqslant r<\frac{1}{2}d}\left(\frac{d}{d-r}\right)=\sum_{\frac{1}{2}d<r\leqslant d-1}\left(\frac{d}{r}\right)$$

又因为d为偶数时，$\left(\frac{d}{d/2}\right)=0$，故有

$$2\sum_{1\leqslant r\leqslant\frac{1}{2}d}\left(\frac{d}{r}\right)=2\sum_{\frac{1}{2}d<r\leqslant d-1}\left(\frac{d}{r}\right)$$

$$=\sum_{r=1}^{d-1}\left(\frac{d}{r}\right)=0 \qquad (4)$$

再由（3）得 $$\sum_{r=1}^{d-1}\left(\frac{d}{r}\right)r=0 \qquad (5)$$

从（4）、（5）立得

$$|d|\sum_{r=1}^{[\frac{1}{2}|d|]}\left(\frac{d}{r}\right)=\left(\left(\frac{d}{2}\right)-2\right)\sum_{r=1}^{|d|}\left(\frac{d}{r}\right)r.$$

说明 原题将所要证明的等式误为

$$|d|\sum_{r=1}^{[\frac{1}{2}|d|]}\left(\frac{d}{r}\right)=\left(2-\left(\frac{d}{2}\right)\right)\sum_{r=1}^{|d|}\left(\frac{d}{r}\right)r.$$

习题2 设$p\equiv 3 \pmod 4$，则于0，$\frac{1}{2}p$之间二次剩余之个数多于非二次剩余之个数；若$p\equiv 1 \pmod 4$，则其数相等。

证：要证明$p\equiv 3\pmod 4$时，0、$\frac{1}{2}p$之间二次剩余的个数多于非二次剩余的个数，只需证明

$$\sum_{r=1}^{\frac{1}{2}(p-1)}\left(\frac{r}{p}\right)\geqslant 1$$

即可．设$d=-p$，由于$p\equiv 3\pmod 4$、$d\equiv 1\pmod 4$，因为d为一负的基本判别式，由12.12.4得

$$\sum_{r=1}^{\left[\frac{|d|}{2}\right]}\left(\frac{d}{r}\right)=\frac{2\left(2-\left(\frac{d}{2}\right)\right)h(d)}{w} \tag{1}$$

由12．3．1得 $\left(\frac{d}{r}\right)=\left(\frac{r}{|d|}\right)=\left(\frac{r}{p}\right)$

其中$\left(\frac{d}{r}\right)$为Kronecker符号，$\left(\frac{r}{p}\right)$为Legendre符号．又因为Kronecker符号

$$\left(\frac{d}{2}\right)=\left(\frac{-p}{2}\right)=\begin{cases}1, & \text{当}-p\equiv 1\pmod 8\text{时}\\ -1, & \text{当}-p\equiv 5\pmod 8\text{时}\end{cases}$$

且$w=2$（由11．4．3），类数$h(d)=h(-p)\geqslant 1$．

$$\left[\frac{|d|}{2}\right]=\left[\frac{p}{2}\right]=\frac{1}{2}(p-1)．$$

故由（1）有

$$\sum_{r=1}^{\frac{1}{2}(p-1)}\left(\frac{r}{p}\right)=(2\pm 1)h(-p)\geqslant 1$$

此即当$p\equiv 3\pmod 4$时，0、$\frac{1}{2}p$之间二次剩余的个数多于非二次

剩余的个数。

欲证 $p\equiv 1\ (\text{mod}4)$ 时，0、$\frac{1}{2}p$ 之间二次剩余个数与二次非剩余个数相等，只需证明 $\sum_{r=1}^{\frac{1}{2}(p-1)}\left(\frac{r}{p}\right)=0$ 即可。因为

$$\sum_{r=1}^{\frac{1}{2}(p-1)}\left(\frac{r}{p}\right)=\sum_{r=1}^{\frac{1}{2}(p-1)}\left(\frac{-r}{p}\right)=\sum_{r=-1}^{-\frac{1}{2}(p-1)}\left(\frac{r}{p}\right)$$

$$=\sum_{r=-1}^{-\frac{1}{2}(p-1)}\left(\frac{p+r}{p}\right)=\sum_{r=\frac{1}{2}(p+1)}^{p-1}\left(\frac{r}{p}\right)$$

并且 $$\sum_{r=1}^{p-1}\left(\frac{r}{p}\right)=\sum_{r=1}^{\frac{1}{2}(p-1)}\left(\frac{r}{p}\right)+\sum_{r=\frac{1}{2}(p+1)}^{p-1}\left(\frac{r}{p}\right)=0$$

故 $$2\sum_{r=1}^{\frac{1}{2}(p-1)}\left(\frac{r}{p}\right)=0$$

$$\sum_{r=1}^{\frac{1}{2}(p-1)}\left(\frac{r}{p}\right)=0$$

此即 $p\equiv 1\ (\text{mod}4)$ 时，0、$\frac{1}{2}p$之间二次剩余个数与二次非剩余个数相等。

第十三章　模变换

一、提　　要

定义　对应于一线性变换A：

$$z'=\frac{az+b}{cz+d}$$

有一方阵

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

此方阵的行列式的值$ad-bc$（$\neq 0$），称为此变换的行列式。

定义　若一组线性变换其中包有单位变换（$z'=z$），且其中二变换的积仍在其中，任一变换的逆变换也在其中，则此组变换组成一群。

定义　若z_0由A变为其自己，则称此点为A的定点。

定义　若有一变换连续使用若干次而成为单位变换，则称它为有限次变换，使其成为单位变换的最小次数，称为该变换的周期。

定义

$$(z_1z_2z_3z_4)=\frac{z_3-z_1}{z_2-z_3}\Big/\frac{z_4-z_1}{z_2-z_4}$$

称为四点z_1、z_2、z_3、z_4的交比。

定理 1　线性变换使交比不变。

定理 2　线性变换使二园的交角不变。

定义　若a、b、c、d是整数，且

$$ad-bc=1,$$

则变换

$$z'=\frac{az+b}{cz+d}$$

称为模变换。

定义　上半平面上的二点z、z'，如能有一模变换将z变为z'，则称此二点相似，用$z\sim z'$表示。

显然有

(*i*)　$z\sim z$；

(*ii*)　若$z\sim z'$，则$z'\sim z$；

(*iii*)　若$z\sim z'$，$z'\sim z''$，则$z\sim z''$。

定义　上半平面的区域

$$D:\begin{cases}-\dfrac{1}{2}\leqslant x<\dfrac{1}{2},\\ x^2+y^2>1,\ \text{当}x>0\text{时},\\ x^2+y^2\geqslant 1,\ \text{当}x\geqslant 0\text{时};\end{cases}$$

称为基域，在D上的点称为既约点。

定理 3　无二既约点可以彼此相似。

定理 4　在长方形$-\frac{1}{2}\leqslant x<\frac{1}{2}$，$y\geqslant\gamma$（$\gamma\geqslant 0$）中，相似于一定点的点数有限。也就是将长方形中的点分为相似点组，则每组中的点数有限。

定理5　上半平面的任一点，相似于唯一的既约点。

二、题　　解

§ 6　基　　域

习题 1　凡$z=\frac{a+i}{c}$，$a^2+bc+1=0$，皆相似于i。

证： 由相似定义知道$\frac{a+i}{c}$是上半平面内的点，因此$c>0$。再由已知条件$a^2+bc+1=0$知道$b\leqslant -1$。设$b=-b'$，$b'\geqslant 1$，$a^2+bc+1=0$变为$a^2-b'c+1=0$。

（一）　当$b'=1$时，从

$$\frac{a+i}{a^2+1}=\frac{i}{1+ai}$$

此时$c=a^2+1$，$b=-1$，$a^2+bc+1=0$知道

$$\frac{a+i}{c}\sim i.$$

（二）　当$b'>1$时，由$a^2-b'c+1=0$知道，对任意有理素数$p\mid c$，一定有$p\equiv 1 \pmod 4$，否则$p\equiv 3 \pmod 4$，$a^2\equiv -1 \pmod p$与$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=-1$相矛盾。

当$2\mid a$时，$-b'c+1\equiv 0 \pmod 4$，$b'c\equiv 1 \pmod 4$，得$c\equiv \pm 1 \pmod 4$。再由前证，$c\equiv 1 \pmod 4$。因若$c\equiv 3 \pmod 4$，则必有有理素数$q\mid c$，$q\equiv 3 \pmod 4$，此不可能。

当$2\nmid a$时，$1-b'c+1\equiv 0\pmod 4$，$b'c\equiv 2\pmod 4$，$c\equiv 1$，$2\pmod 4$。

从前所述，我们可设c的分解式为

$$c=2^t p_1^{a_1}\cdots p_l^{a_l}$$

其中$p_j\equiv 1\pmod 4$，$1\leqslant j\leqslant t$，$t=0$或者1。因此，对于c的每个奇素数因子p_j（$1\leqslant j\leqslant l$），可找到有理整数X_j、Y_j，使得

$$p_j=X_j^2+Y_j^2,\quad (X_j,\ Y_j)=1$$

再据恒等式

$$2(X^2+Y^2)=(X+Y)^2+(X-Y)^2$$

$$(X^2+Y^2)(X'^2+Y'^2)=(XX'+YY')^2+(XY'-YX')^2$$

知道存在有理整数y_1、y_2，使得

$$c=y_1^2+y_2^2.$$

（由第12章提要中定理11：$x^2+y^2=k$的解数为四倍于k的因数$\equiv 1\pmod 4$的个数，减去k的因数$\equiv 3\pmod 4$的个数。c的素因子$\equiv 1\pmod 4$也可证明此点）。所以，在复整数环

$$Z(i)=\{a+bi\,|\,a,\ b\text{是有理整数}\}$$

中有

$$(a+i)(a-i)=b'c=b'(y_1^2+y_2^2)$$
$$=b'(y_1i+y_2)(-y_1i+y_2)\qquad(1)$$

设$(a+i,\ a-i)=d$，则$d\,|\,2i$，$d=1$或2。如果$d=2$，则有$ei+f\in Z(i)$，使得$a\pm i=2(\pm ei+f)$，从而$1=2e$，此不可能。因此，$(a+i,\ a-i)=1$（舍去结合数）。

设y_1i+y_2的素分解式为

$$y_1i+y_2=\prod_{r=1}^{s}(a_ri+b_r)$$

则$-y_1i+y_2$的素分解式为

$$-y_1 i+y_2=\prod_{r=1}^{s}(-a_r i+b_r)$$

其中每个素因子允许重复.于是，（1）可写成

$$(a+i)(a-i)=b'\prod_{r=1}^{s}(a_r i+b_r)\cdot\prod_{r=1}^{s}(-a_r i+b_r) \qquad (2)$$

由于$a+i$和$a-i$互素，它们的素因子共轭成对且个数相同，$y_1 i+y_2$和$-y_1 i+y_2$的素因子也是共轭成对且个数相同，因此我们可以适当地交换（2）式右端各素因子的顺序，把（2）写成

$$(a+i)(a-i)=b'\prod_{r=1}^{s}(a_r' i+b_r')\prod_{r=s+1}^{2s}(a_r i+b_r) \qquad (3)$$

且合条件 $$\prod_{r=1}^{s}(a_r' i+b_r')\Big|a+i$$

$$\prod_{r=s+1}^{2s}(a_r i+b_r)\Big|a-i$$

而$a_r' i+b_r'$（$1\leqslant r\leqslant s$）和$a_r i+b_r$（$s+1\leqslant r\leqslant 2s$）都取自$\pm a_r i+b_r$（$1\leqslant r\leqslant s$）之中.

如果命 $$\prod_{r=1}^{s}(a_r' i+b_r')=y_1' i+y_2' \qquad (4)$$

结合$c=(y_1 i+y_2)(-y_1 i+y_2)$可得

$$\prod_{r=s+1}^{2s}(a_r i+b_r)=-y_1' i+y_2' \qquad (5)$$

把（4）、（5）代入（3）得

$$(a+i)(a-i)=b'(y_1' i+y_2')(-y_1' i+y_2')$$

从$y_1' i+y_2'\mid a+i$可找到整数$x_1' i+x_2'\in Z(i)$，使得

$$a+i=(x_1' i+x_2')(y_1' i+y_2') \qquad (6)$$

比较虚部系数得

$$x_1'y_2'+x_2'y_1'=1 \tag{7}$$

（6）两端同时除以$c=(y_1'i+y_2')(-y'_1i+y_2')$得

$$\frac{a+i}{c}=\frac{x_1'i+x_2'}{-y_1'i+y_2'}$$

结合（7）式，立得

$$\frac{a+i}{c}\sim i.$$

说明： 由于$Z(i)$中任意二元素的和，差，积仍在$Z(i)$中，因此$Z(i)$成一环，一般称为Gauss整环。设α，β是$Z(i)$中的两个元素，若有$\gamma\in Z(i)$，使$\alpha=\beta\gamma$，则称β可整除α，并且记成$\beta|\alpha$，否则称β不能整除α，记成$\beta\nmid\alpha$。若α只被自己和单位± 1，$\pm i$整除，则称α为$Z(i)$中的素数或不可分数。如果$Z(i)$中的两个元素只差一个单位因子，则称它们为结合数。

习题2 凡

$$z=\frac{a+\rho}{c},\ a(1-a)-bc=1$$

皆相似于ρ。

证： 由相似定义立得$c>0$。$c=1$时结论显然成立，故可设$c>1$。$a(1-a)-bc=1$就是$a^2-a+1=-bc$。由$a^2-a+1>0$，$c>1$可知$-b>0$。设$-b=b'$，得

$$a^2-a+1=b'c,\ b'>0.$$

（一） 当$b'=1$时

$$\frac{a+\rho}{c}=\frac{\rho}{a\rho+1}$$

此时$c=a^2-a+1$，$b=-1$，$\frac{a+\rho}{c}\sim\rho$。

（二） 当$b'>1$时，从

$$a^2-a+1=(a+\rho)(a+\rho^2)$$

得
$$(a+\rho)(a+\rho^2)=b'c \quad (1)$$

i) 先证$a+\rho$与$a+\rho^2$互素．设$(a+\rho,\ a+\rho^2)=d$，$d|\rho^2(a+\rho)-\rho^2(a+\rho^2)=1-\rho$．由于$1-\rho$是$Z(\rho)$中的素数，故$d=1$或$1-\rho$（舍去结合数）．若$d=1-\rho$，则$1-\rho|a+\rho$；由于$1-\rho$与$1-\rho^2$共轭，$a+\rho$与$a+\rho^2$共轭，因此$1-\rho^2|a+\rho^2$．同理，从$1-\rho|a+\rho^2$可得$1-\rho^2|a+\rho$．故$1-\rho^2|d=1-\rho$，$1+\rho|1$，此不可能．

ii)再证c必可表成$Z(\rho)$中一对共轭整数的乘积．由于$Z(\rho)$中整数形如$d\rho+f$，d、f是有理整数．又$\bar{\rho}=\rho^2$，$\rho=-\rho^2-1$，因而只需证明

$$c=(y_1\rho+y_2)(y_1\rho^2+y_2)$$．

即可．其中y_1、y_2是有理整数．显然$c\neq q$，q是有理素数且$q\equiv 2 \pmod 3$；否则$c=q$为$Z(\rho)$中的素数，由（1）得$q|a+\rho$，$\bar{q}|a+\rho^2$或$q|a+\rho^2$，$\bar{q}|a+\rho$．但$\bar{q}=q$，从而该两种情形均给出$q|(a+\rho,\ a+\rho^2)$，与$(a+\rho,\ a+\rho^2)=1$矛盾．因此可设

$$c=(a_1\rho+a_2)(b_1\rho^2+b_2)$$

比较上式虚部和实部得

$$a_1b_2=a_2b_1 \quad (2)$$

$$2c=2a_1b_1-a_1b_2-a_2b_1+2a_2b_2 \quad (3)$$

由（2）可设 $\frac{a_1}{a_2}=\frac{b_1}{b_2}=\frac{B_1}{A_1}$，$(B_1,\ A_1)=1$

代入（3）得

$$c=\left(\frac{B_1^2}{A_1^2}-\frac{B_1}{A_1}+1\right)a_2b_2=\left(\frac{B_1}{A_1}+\rho\right)\cdot$$

$$\left(\frac{B_1}{A_1}+\rho^2\right)a_2b_2=\frac{1}{A_1{}^2}(B_1+A_1\rho)(B_1+A_1\rho^2)a_2b_2 \qquad (4)$$

从 $(B_1, A_1)=1$ 得

$$(A_1,B_1+A_1\rho)=(A_1, B_1+A_1\rho^2)=1.$$

由（4）得$A_1{}^2|a_2b_2$。设$a_2b_2=C_1A_1{}^2$，代入（4）得

$$c=(B_1+A_1\rho)(B_1+A_1\rho^2)C_1$$

如果c不能写成$Z(\rho)$中二共轭整数的乘积，则必存在自然数n，把上面的方法使用n次后可得

$$c=(B_1+A_1\rho)(B_1+A_1\rho^2)\cdots(B_n+A_n\rho)$$
$$(B_n+A_n\rho^2)C_n \qquad (5)$$

（5）中有理整数C_n不可化且诸有理整数A_1，$\cdots A_n$，B_1，$\cdots B_n$合条件

$$(B_1, A_1)=\cdots=(B_n, A_n)=1$$

显然$C_n\neq 1$，否则由（5）c可表成两个共轭整数的乘积，与C不可表成两个共轭整数乘积的假设相矛盾。故$C_n=p$，p为有理素数且$p\equiv 2 \pmod 3$。如前所证，从（1）得$p|(a+\rho,a+\rho^2)$与$(a+\rho, a+\rho^2)=1$矛盾。

综上所述，c一定能写成两个共轭整数的乘积，即存在有理整数y_1、y_2，使得

$$c=(y_1\rho+y_2)(y_1\rho^2+y_2) \qquad (6)$$

把（6）代入（1）得

$$(a+\rho)(a+\rho^2)=b'(y_1\rho+y_2)(y_1\rho^2+y_2).$$

与习题1证明过程中所述理由相同，不妨设

$$y_1\rho+y_2|a+\rho^2 \qquad (7)$$
$$y_1\rho^2+y_2|a+\rho$$

或

$$y_1\rho+y_2|a+\rho \qquad (8)$$
$$y_1\rho^2+y_2|a+\rho^2$$

如果（7）成立，由$y_1\rho^2+y_2|a+\rho$知存在整数$x_1\rho+x_2\in Z(\rho)$，使得

$$a+\rho=(x_1\rho+x_2)(y_1\rho^2+y_2) \qquad (9)$$

比较上式两端虚部得

$$x_1y_2-x_2y_1=1 \qquad (10)$$

（9）式两端同除以$c=(y_1\rho+y_2)(y_1\rho^2+y_2)$得

$$\frac{a+\rho}{c}=\frac{x_1\rho+x_2}{y_1\rho+y_2}$$

结合（10）立得 $\quad \frac{a+\rho}{c}\sim\rho$

如果（8）成立，由$y_1\rho+y_2|a+\rho$，$y_1\rho+y_2=y_1'\rho^2+y_2'$（此处$y_1'=-y_1$，$y_2'=y_2-y_1$），知存在整数$x_1'\rho+x_2'\in Z(\rho)$，使得

$$a+\rho=(x_1'\rho+x_2')(y_1'\rho^2+y_2') \qquad (11)$$

上式同样给出 $\quad x_1'y_2'-x_2'y_1'=1 \qquad (12)$

（11）式两端同除以$c=(y_1'\rho+y_2')(y_1'\rho^2+y_2')$得

$$\frac{a+\rho}{c}=\frac{x_1'\rho+x_2'}{y_1'\rho+y_2'}$$

结合（12）得 $\quad \frac{a+\rho}{c}\sim\rho$

由（一）、（二）可知，凡 $\quad z=\frac{a+\rho}{c}$，$a(1-a)-bc=1$皆相似于ρ。

说明： $Z(\rho)$表所有形如$d\rho+f$的数，其中d和f是有理整数。$Z(\rho)$显然成一环。设α、β是$Z(\rho)$中的元素。如果有$\gamma\in Z(\rho)$，使得$\alpha=\beta\gamma$，则称β可整除α，记为$\beta|\alpha$，否则，称β不能整除α，记为$\beta\nmid\alpha$。若α只被自己和单位±1、$\pm\rho$、$\pm\rho^2$整除，则称α为$Z(\rho)$中的素数或不可分数。如果$Z(\rho)$中两个元素只差一个单位因子，

则称它们为结合数。

§9 二次定正型

习题1 定出经一非单位模变换而不变的二次型之标准形式（答：x^2+y^2，x^2+xy+y^2）。

此题有误，其原因如下：

i）题目中“经一非单位模变换”，如果是指“任一非单位模变换”，则此时我们能证明如下结论：经任一非单位模变换而不变的非零二次型是不存在的。下面就用反证法来证明此结论。

如果存在一个二次型

$$F(x,\ y)=Ax^2+Bxy+Cy^2$$

它经任一非单位模变换均不变；$F(x,\ y)\neq 0$，A、B、C为整数。把$F(x,\ y)$写成

$$F(x,\ y)=(y,\ y)\begin{pmatrix}A & B\\ 0 & C\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix} \qquad (1)$$

设
$$\begin{pmatrix}x\\ y\end{pmatrix}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}x'\\ y'\end{pmatrix} \qquad (2)$$

则
$$(x,\ y)=(x',\ y')\begin{pmatrix}a & c\\ b & d\end{pmatrix} \qquad (2')$$

其中a、b、c、d都是整数，且合条件

$$ad-bc=1,\ a\neq d,\ b\neq -c,\ abcd\neq 0.$$

显然（2）是一个非单位的模变换。由假定知道，$F(x,y)$在变换（2）下是不变的。把（2）、（2′）代入（1）得

$$F(x,\ y)=(x',\ y')\begin{pmatrix}a & c\\ b & d\end{pmatrix}\begin{pmatrix}A & B\\ 0 & C\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}x'\\ y'\end{pmatrix}$$

$$=(x',\ y')\begin{pmatrix}a^2A+acB+c^2C & abA+adB+cdC\\ abA+bcB+cdC & b^2A+bdB+d^2C\end{pmatrix}\begin{pmatrix}x'\\ y'\end{pmatrix}$$

则二次型$F(x, y)$在非单位模变换（2）下不变的充分必要条件是

$$\begin{cases} a^2A + acB + c^2C = A \\ abA + bcB + cdC = 0 \\ abA + adB + cdC = B \\ b^2A + bdB + d^2C = C \end{cases} \qquad (3)$$

或

$$\begin{cases} a^2A + acB + c^2C = C \\ abA + bcB + cdC = 0 \\ abA + adB + cdC = B \\ b^2A + bdB + d^2C = A \end{cases} \qquad (3')$$

下面只讨论（3），因为（3′）同理可证。

由于$ad - bc = 1$，所以（3）可以写为

$$\begin{cases} (a^2 - 1)A + acB + c^2C = 0 \\ abA + bcB + cdC = 0 \\ b^2A + bdB + (d^2 - 1)C = 0 \end{cases} \qquad (3)$$

用b^2乘第一式，减去$(a^2 - 1)$乘第三式得

故得 $$\begin{cases} abA + bcB + cdC = 0 \\ bB + (d - a)C = 0 \end{cases}$$

$$\begin{cases} A = \dfrac{-c}{a-d}B \\ C = \dfrac{b}{a-d}B \end{cases} \qquad (4)$$

由于$ad - bc = 1$，所以方程$aX - bY = 1$的所有解由下式给出：

$$\begin{cases} X = d + bt \\ Y = c + at \end{cases}$$

其中t是任意整数．我们可以选取t，使得有$|a - X| > |bB|$．另外，

$$\begin{pmatrix} a & b \\ Y & X \end{pmatrix}$$

也是一模方阵，由假定知道$F(x、y)$在它的作用下也是不变的。因此，从（4）可得

$$\begin{cases} A=\dfrac{-Y}{a-X}B \\ C=\dfrac{b}{a-X}B \end{cases} \qquad (4')$$

由于C是整数，从而由（4′）得出$a-X|bB$，但是$|a-X|>|bB|$，故有$B=0$或$b=0$，均与前设相矛盾。

例： 答案中的x^2+y^2在变换$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$下是不变的，但在变换$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$下就变为$x^2+2xy+2y^2$。

从i）容易得出结论：二次型$F(x, y)$经任一非单位模变换不变的充分必要条件是$F(x、y)$恒为零。

ii）"经一非单位模变换"如果是指某一非单位模变换的此话，此变换应当作为已知条件给出。否则，可选取变换$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$。显然，$x^2+y^2$，$Ax^2+Ay^2$（$A$非平方数）在该变换下都不变，但$Ax^2+Ay^2$却不在答案之中。

由i）、ii）可知，此题不妨改为：二次型$F(x, y)$经任一非单位模变换不变的充分必要条件是$F(x, y)$恒为零。

第十四章　整数矩阵及其应用

一、提　　要

定义　称

$$A=\begin{pmatrix} a_{11} & a_{12}\cdots a_{1n} \\ a_{21} & a_{22} \quad a_{2n} \\ \cdots\cdots & \cdots\cdots \\ a_{m1} & a_{m2}\cdots a_{mn} \end{pmatrix}$$

为m行n列矩阵，或$m\times n$矩阵，用$A^{(m,n)}$表示。如果$m=n$，则称A为n级方阵，用$A^{(n)}$或(a_{ij})表示。其中$a_{11},a_{12},\cdots,a_{mn}$都是整数。

定义　1)　二方阵$A=(a_{ij})$，$B=(b_{ij})$的和为：

$$A+B=(a_{ij}+b_{ij})\ ;$$

2)　设

$$B=\begin{pmatrix} b_{11}\cdots\cdots b_{1l} \\ b_{21}\cdots\cdots b_{2l} \\ \cdots\cdots\cdots\cdots \\ b_{n1}\cdots\cdots b_{nl} \end{pmatrix}$$

矩阵A、B的乘积为

$$AB=C=\begin{pmatrix} c_{11}\cdots\cdots c_{2l} \\ c_{21}\cdots\cdots c_{1l} \\ \cdots\cdots\cdots\cdots \\ c_{m1}\cdots\cdots c_{ml} \end{pmatrix},$$

其中 $c_{ij}=\sum_{t=1}^{n}a_{it}b_{tj}$，$i=1,\cdots,m$；$j=1,\cdots,l$。

定义 方阵$A^{(\ )}$中除去第i行第j列上的元素，但不变动其它元素位置所得（$n-1$）级方阵的行列式，称为a_{ij}的余子式；余子式前面添加符号$(-1)^{i+j}$后，称为代数余子式，用A_{ij}表示。

定义 称

$$A_0=\begin{pmatrix} A_{11}\cdots\cdots A_{n1} \\ A_{12}\cdots\cdots A_{n2} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ A_{1n}\cdots\cdots A_{nn} \end{pmatrix}$$

为$A=A^{(n)}$的伴随矩阵。

定理 1 $AA_0=A_0A=aI$，其中$a=|A|$，I为单位矩阵。

定义 如果方阵A的行列行$|A|=\pm 1$，则称A为模方阵；如果$|A|=1$，则称为正模方阵。

定理 2 全体模方阵成为一群；全体正模方阵也成为一群。

定理3 全体模方阵所成的群，可由U_1、U_2、U_3的乘方与乘积表出。其中

$$U_1=\begin{pmatrix} 0 & 0\cdots\cdots 0 & (-1)^{n-1} \\ 1 & 0\cdots\cdots 0 & 0 \\ \cdots\cdots & \cdots\cdots\cdots\cdots & \cdots\cdots \\ 0 & 0\cdots\cdots 1 & 0 \end{pmatrix}$$

$$U_2=\begin{pmatrix} 1 & 1 & 0\cdots 0 \\ 0 & 1 & 0\cdots 0 \\ 0 & 0 & 1\cdots 0 \\ \cdots & \cdots & \cdots\cdots \\ 0 & 0 & 0\cdots 1 \end{pmatrix},\quad U_3=\begin{pmatrix} -1 & 0 & 0\cdots 0 \\ 0 & 1 & 0\cdots 0 \\ \cdots & \cdots & \cdots\cdots \\ 0 & 0 & 0\cdots 1 \end{pmatrix}.$$

定理4 正模方阵所成的群$\mathbf{M}_n$可由U_1、U_2的乘方与乘积

表出。

定义 若有一模方阵U，使二方阵A、B间关系$A=UB$,则称方阵B左结合于方阵A，并以$A\overset{L}{=}B$表示。

定理 5 任一方阵必左结合于如下形式的方阵

$$B=\begin{pmatrix} b_{11} & 0 & 0 \cdots\cdots\cdots 0 & 0 \\ b_{21} & b_{22} & 0 \cdots\cdots\cdots 0 & 0 \\ \cdots\cdots & \cdots\cdots & \cdots\cdots\cdots\cdots\cdots & \cdots \\ b_{\ -1\,1} & b_{\ -1\,2} & b_{\ -1\,3} \cdots\cdots b_{\ -1\ -1} & 0 \\ b_{\ 1} & b_{\ 2} & b_{\ 3} \cdots\cdots\cdots b_{nn-1} & b_{nn} \end{pmatrix}. \qquad (1)$$

其中$b_{\nu\nu}\geqslant 0$，且若$b_{\nu\nu}>0$，则

$$0\leqslant b\ < b\quad (i>\nu)\ .$$

定义 形如（1）的方阵称为左结合标准形。

定义 对二矩阵$A=A^{(\ ,\ n)}$，$B=B^{(m,\ n)}$，若有二模方阵$U=U^{(m)}$，$V=V^{(n)}$，使得

$$A=UBV,$$

则称A与B相似，记为$A\sim B$。

定理 6 任一矩阵$A=A^{(m,\ n)}$，必与形如

$$\begin{pmatrix} d_1 & 0 & 0 \cdots\cdots\cdots\cdots 0 \cdots\cdots 0 \\ 0 & d_1d_2 & 0 \cdots\cdots\cdots\cdots 0 \cdots\cdots 0 \\ 0 & 0 & d_1d_2d_3 \cdots\cdots\cdots 0 \cdots\cdots 0 \\ \cdots\cdots & \cdots\cdots & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ 0 & 0 & 0 \cdots\cdots d_1d_2\cdots d_m \cdots 0 \end{pmatrix} \quad (m\leqslant n) \qquad (2)$$

或

$$\begin{pmatrix} d_1 & 0 \cdots\cdots\cdots 0 \\ 0 & d_1d_2 \cdots\cdots 0 \\ \cdots\cdots & \cdots\cdots\cdots\cdots \\ 0 & 0 \cdots d_1d_2\cdots d_n \\ 0 & 0 \cdots\cdots\cdots 0 \\ \cdots\cdots & \cdots\cdots\cdots\cdots \\ 0 & 0 \cdots\cdots\cdots 0 \end{pmatrix} \quad (m\geqslant n) \qquad (3)$$

的矩阵相似，其中$d_i \geqslant 0$.

定义 形如（2）或（3）的矩阵，称为相似标准形.

定理 7 若$A \sim B$，则A内所有i行i列子行列式的最大公因数，与B内所有i行i列子行列式的最大公因数相等.

定理 8 任一矩阵的相似标准形，一定是唯一的.

定义 在矩阵A的相似标准形（2）或（3）中，对角线上不为零的元素

d_1，$d_1 d_2$，…，$d_1 \cdots d_k$，$(k \leqslant \min(m, n))$分别称为A的1次，2次，…k次不变因子. k称为矩阵A的秩，不变因子的标准分解式

$$d_1 \cdots d = p_1^{e_{i1}} \cdots p_{l_i}^{e_{il_i}}$$

$$(e_{ij} > 0, \quad 1 \leqslant i \leqslant k, \quad l_{i-1} \leqslant l_i)$$

中，所有的素数幂$p_j^{e_{ij}}$都称为A的初等因子.

定理 9 $A \sim B$的充分必要条件是A、B有相同的秩和相同的初等因子.

定理10 方程组

$$y_i = \sum_{j=1}^{n} a_{ji} x_j, \quad (1 \leqslant i \leqslant m, \quad n \geqslant m)$$

有解的充分必要条件是二矩阵A及$\begin{pmatrix} A \\ y \end{pmatrix}$有相同的不变因子.

定义 对于二方阵A、B，如有一方阵C使$A = CB$，则称B为A的右因子，或B右除尽A，用$B | A$表示.

定义 设A非奇异方阵，也非模方阵. 若对A的任何分解式$A = BC$都有B或C是模方阵，则称A为不可分解方阵或素方阵；不然，称A为复合方阵.

定理11 一方阵为素方阵的充分必要条件是其行列式为素数.

定理12 任一复合方阵可以分解成有限多个素方阵的乘积，

且其因子数等于其行列式的素因子数。

定义 若一素方阵可以表为如下形式：

$$U^{-1}[1, \cdots, 1, p]U$$

则此素方阵称为标准素方阵；U是一模方阵。

定义 对一非奇异方阵A，适合于

$$A \cup A_0 \equiv O \pmod{|A|}$$

的模方阵U称为A的伴随模方阵。A_0是A的伴随方阵，$|A|$表A的行列式的绝对值。

定理13 A的伴随模方阵成一群。

定义 A的伴随模方阵所成的群，称为A的伴随模群。

定义 如果方阵D为方阵A及B（A与B不同时为O）的右公因子，且A、B的任何右公因子都是D的右因子，则称D为A、B的右最大公约。

定理14 不同时为0的二方阵A、B必有最大公约D，且存在方阵P及Q，使

$$PA+QB=D.$$

定理15 二非奇异方阵A，B必有一最小公倍M存在，且M非奇异，而其它的最小公倍都形如UM。此处U为模方阵。

定理16 设方阵B非奇异，则对任一方阵A，必存在二方阵Q及C，使

1） $A=QB$；

或

2） $A=QB+C$，$0<|C|<|B|$。

定义 命x_1，…，x_n表n个未定量。所有的整系数一次式

$$y=a_1x_1+\cdots+a_nx_n$$

成一集合，该集合用$\mathbf{O}=\{x_1, \cdots x_n\}$表示。

定义 如果$y'=a_1'x_1+\cdots+a_n'x_n$，则定义$y\pm y'$为

$$y\pm y'=(a_1\pm a_1')x_1+\cdots+(a_n\pm a_n')x_n.$$

定义　O中的一个子集合M如有以下性质则称为模：若y_1、y_2在M中，则$y_1 \pm y_2$也在M中。

定义　如M中有一组元素y_1，…，y_l，使M内任一元素都可唯一地表为

$$b_1 y_1 + \cdots + b_l y_l$$

的形式，其中b_1，…b_l是整数，则y_1，…，y_l称为M的底，l称为M的维数。

定理17　模必有底，维数$\leqslant n$。

定理18　模的维数与底的选择无关。

定理19　n维模M必有如下形式的基底

$$\begin{aligned} y_1 &= a_{11}x_1 \\ y_2 &= a_{21}x_1 + a_{22}x_2 \\ &\cdots\cdots \\ y_n &= a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \end{aligned}$$

其中

$$a_{\nu\nu} > 0 \quad (1 \leqslant \nu \leqslant n)，且 0 \leqslant a_{\mu\nu} < a_{\nu\nu} \quad (\mu > \nu)。$$

定义　以上形式的基底称为标准基底。

二、题　解

§1　引　言

习题　读者自己研究奇异方阵之情况。

解：本节定理4指明任一二阶非奇异方阵的左结合标准形是唯一的。该题要求讨论二阶奇异方阵的左结合标准形是否唯一。下面证明奇异方阵

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

的左结合标准形并不唯一。

（一） 当$\begin{pmatrix} A & B \\ C & D \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$时，如果$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$与$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$左结合，则一定存在一个模方阵$\begin{pmatrix} r & s \\ u & v \end{pmatrix}$，使得

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} r & s \\ u & v \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

由矩阵乘法，对于任意整数k，均有

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} r & s \\ u & v \end{pmatrix}\begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix}$$

此即 $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$与$\begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix}$

左结合。故此种情形$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$的左结合标准形并不唯一。

（二） 当$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\neq\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$时，由提要中定理 5 知，$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$左结合形如$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$的方阵；再由$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$的奇异性可知$a$、$d$中至少有一个是零。

1.如果$c\neq 0$

(i) 当$a=d=0$时，取模方阵$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

由

$$\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ -c & 0 \end{pmatrix}$$

知道$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$又与$\begin{pmatrix} 0 & 0 \\ -c & 0 \end{pmatrix}$左结合；但$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$与$\begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}$也是左结合的，因而此种情形，$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$左结合标准形不唯一.

ii) 当$a=0$, $d\neq 0$时，仍然取模方阵$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$，从

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ -c & -d \end{pmatrix}$$

便知$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$又与$\begin{pmatrix} 0 & 0 \\ -c & -d \end{pmatrix}$左结合.

(iii) 当$a\neq 0$, $d=0$时，取模方阵

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

从$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}=\begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix}=\begin{pmatrix} -a & 0 \\ c & 0 \end{pmatrix}$

知道$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$又与$\begin{pmatrix} -a & 0 \\ c & 0 \end{pmatrix}$左结合.

2. 如果$c=0$, $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}=\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$.

(i) 当$a=d=0$时，方阵$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$变成零方阵$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$，此时

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\text{与}\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

左结合，于是存在一个模方阵M，使得

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}=M\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

故 $$\begin{pmatrix} A & B \\ C & D \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

与 $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ 相矛盾。

(ii) 当$a=0$，$d\neq 0$时。由

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix}$$

$$=\begin{pmatrix} 0 & 0 \\ 0 & -d \end{pmatrix}$$

知道，$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ 又与 $\begin{pmatrix} 0 & 0 \\ 0 & -d \end{pmatrix}$ 左结合。

(iii) 当$a\neq 0$，$d=0$时。由

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}=\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

$$=\begin{pmatrix} -a & 0 \\ 0 & 0 \end{pmatrix}$$

知道 $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ 又与 $\begin{pmatrix} -a & 0 \\ 0 & 0 \end{pmatrix}$ 左结合。

综上所述，奇异方阵

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

的左结合标准形并不唯一。

§4 左结合

习题 证明非奇异方阵之左结合标准形式是唯一的。

证：对任一方阵M，由定理5可知，必左结合如下形式的方

阵：

$$B=\begin{pmatrix} b_{11} & 0 & 0\cdots\cdots & 0 & 0 \\ b_{21} & b_{22} & 0\cdots\cdots & 0 & 0 \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots \\ b_{n-11} & b_{n-12} & b_{n-13}\cdots\cdots b_{n-1n-1} & & 0 \\ b_{n1} & b_{n2} & b_{n3}\cdots\cdots & b_{nn-1} & b_{nn} \end{pmatrix}$$

其中$b_{vv} \geqslant 0$；且若$b_{vv} > 0$，则$0 \leqslant b_{iv} < b_{vv}$ $(i>v)$，这就是所谓的标准形。由于M是非奇异方阵，故$b_{kk} > 0$ $(k=1, 2, \cdots, n)$，A为任一模方阵。设

$$A=\begin{pmatrix} a_{11} & a_{12}\cdots a_{1n} \\ a_{21} & a_{22}\cdots a_{2n} \\ \cdots\cdots & \cdots\cdots \\ a_{n1} & a_{n2}\cdots a_{nn} \end{pmatrix}=(a_{ij})$$

$$B=\begin{pmatrix} b_{11} & 0 & 0\cdots\cdots & 0 & 0 \\ b_{21} & b_{22} & 0\cdots\cdots & 0 & 0 \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots \\ b_{n-11} & b_{n-12} & b_{n-13}\cdots\cdots & b_{n-1n-1} & 0 \\ b_{n1} & b_{n2} & b_{n3}\cdots\cdots & b_{nn-1} & b_{nn} \end{pmatrix}=(b_{ij})$$

$$B'=\begin{pmatrix} b'_{11} & 0 & 0\cdots\cdots & 0 & 0 \\ b'_{21} & b'_{22} & 0\cdots\cdots & 0 & 0 \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots \\ b'_{n-11} & b'_{n-12} & b'_{n-13}\cdots & b'_{n-1n-1} & 0 \\ b'_{n1} & b'_{n2} & b'_{n3}\cdots\cdots & b'_{nn-1} & b'_{nn} \end{pmatrix}=(b'_{ij})$$

若$AB=B'$，则$A=E$。因为：

（一）方阵A主对角线右上方的所有元素全为零。

将 $b_{kn}=b'_{kn}=0$ $(1\leqslant k\leqslant n-1)$，$b_{nn}>0$

代入 $a_{k1}b_{1n}+a_{k2}b_{2n}+\cdots+a_{kn-1}b_{n-1n}+a_{kn}b_{nn}=b'_{kn}$

得　$a_{kn}=0$，$(1\leqslant k\leqslant n-1)$.　　　　(1)

同理，把$b_{kn-1}=b'_{kn-1}=0$ $(1\leqslant k\leqslant n-2)$，$b_{n-1\,n-1}>0$ 和$a_{kn}=0$代入

$$a_{k1}b_{1n-1}+a_{k2}b_{2n-1}+\cdots+a_{kn-1}b_{n-1\,n-1}+a_{kn}b_{nn-1}=b'_{kn-1}$$

得　$a_{kn-1}=0$，$(1\leqslant k\leqslant n-2)$　　　　(2)

如此使用代入法可以得到

$a_{kn-2}=0$，$(1\leqslant k\leqslant n-3)$

$a_{kn-3}=0$，$(1\leqslant k\leqslant n-4)$

…………………………………

$a_{k3}=0$，$(1\leqslant k\leqslant 2)$　　　　(3)

$a_{k2}=0$，$(k=1)$

由(1)(2)(3)便知，方阵A主对角线右上方的所有元素全为零。

(二) 方阵A主对角线上元素全为1，即$a_{ii}=1$ $(1\leqslant i\leqslant n)$.

由　$|A|=a_{11}a_{22}\cdots a_{nn}=\pm 1$

可知　$a_{ii}=\pm 1$

再由　$a_{ii}b_{ii}=b'_{ii}$，$b_{ii}>0$，$b'_{ii}>0$

得　$a_{ii}=1$

同时也有　$b'_{ii}=b_{ii}$.

(三) 方阵A主对角线左下方的所有元素全为零。把A的第n行与B的第$n-1$列各对应元素相乘得

$$a_{nn-1}b_{n-1\,n-1}+b_{nn-1}=b'_{nn-1}$$

由　$0\leqslant a_{nn-1}b_{n-1\,n-1}+b_{nn-1}=b'_{nn-1}<b'_{n-1\,n-1}=b_{n-1\,n-1}$

且 $b_{n-1\,n-1} > b_{nn-1} \geqslant 0$

得$a_{nn-1}=0$．把A的第n行与B的第$n-2$列各对应元素相乘，并将$a_{nn-1}=0$代入得

$$a_{nn-2}b_{n-2\,n-2}+b_{nn-2}=b'_{nn-2}$$

由 $0 \leqslant a_{nn-2}b_{n-2\,n-2}+b_{nn-2}=b'_{nn-2} < b'_{n-2\,n-2}$

$=b_{n-2\,n-2}$

且 $b_{n-2\,n-2} > b_{nn-2} \geqslant 0$

得$a_{nn-2}=0$．再把A的第n行与B的第$n-3$列各对应元素相乘，并将$a_{nn-1}=a_{nn-2}=0$代入得

$$a_{nn-3}b_{n-3\,n-3}+b_{nn-3}=b'_{nn-3}$$

从而可得$a_{nn-3}=0$．

下面，我们把A的第n行分别与B的第$n-4$、$n-5$、…2、1列各对应元素相乘得到

$$a_{nn-4}=0$$
$$a_{nn-5}=0$$
$$\cdots\cdots\cdots\cdots$$
$$a_{n2}=0$$
$$a_{n1}=0$$

这样，我们就证明了

$$a_{nk}=0\quad(1 \leqslant k \leqslant n-1) \qquad (4)$$

用上面同样的方法，把A的第$n-1$行分别与B的第$n-2$、$n-3$、……2、1列各对应元素相乘，可得到

$$a_{n-1\,n-2}=0$$
$$a_{n-1\,n-3}=0$$
$$\cdots\cdots\cdots\cdots$$
$$a_{n-12}=0$$
$$a_{n-11}=0$$

这就是 $a_{n-1k}=0\quad(1 \leqslant k \leqslant n-2) \qquad (5)$

把A的第$n-2$、$n-3$、……2行分别作与前面类似地处理可得

$$a_{n-2k}=0\quad(1\leqslant k\leqslant n-3)$$
$$a_{n-3k}=0\quad(1\leqslant k\leqslant n-4)$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\qquad(6)$$
$$a_{3k}=0\quad(1\leqslant k\leqslant 2)$$
$$a_{2k}=0\quad(k=1)$$

从（4）、（5）、（6）便知，方阵A主对角线左下方所有元素全为零。

由（一）、（二）、（三）可知$A=E$，因此$AB=B'$给出$B=B'$。故非奇异方阵的左结合标准形式是唯一的。

§7 因子分解.标准素方阵

习题 取$A=[d_1, d_1d_2, \cdots, d_1d_2\cdots d_n]$而研究$A$之伴随模群之性质。

解：设A_0为A的伴随方阵，M为A的伴随模群，方阵

$$U=\begin{pmatrix} U_{11} & U_{12} & \cdots & U_{1n} \\ U_{21} & U_{22} & \cdots & U_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ U_{n1} & U_{n2} & \cdots & U_{nn} \end{pmatrix}$$

为任一模方阵。我们可以证明：$U\in$M的必要充分条件是

$$d_2|U_{12},\ d_2d_3|U_{13},\ d_2d_3d_4|U_{14},\ \cdots,\ d_2d_3\cdots d_n|U_{1n}$$
$$d_3|U_{23},\ d_3d_4|U_{24},\ \cdots d_3\cdots d_n|U_{2n}$$
$$\cdots\cdots\cdots\cdots\qquad(1)$$
$$d_{n-1}|U_{n-2\,n-1},\ d_{n-1}d_n|U_{n-2n}$$
$$d_n|U_{n-1n}$$

本结论的证明由$AUA_0\equiv O(\mathrm{mod}\,|A|)$极易作出。下面以$n=4$示

例。

当$n=4$，时（1）变为：

$$
\begin{aligned}
d_2|U_{12},\ d_2d_3|U_{13},\ &d_2d_3d_4|U_{14}\\
d_3|U_{23},\ &d_3d_4|U_{24}\\
&d_4|U_{34}
\end{aligned}
\qquad (2)
$$

$AUA_0\equiv O(\mathrm{mod}|A|)$给出：

$$
A\cup A_0=\begin{pmatrix} d_1 & & & \\ & d_1d_2 & & \\ & & d_1d_2d_3 & \\ & & & d_1d_2d_3d_4 \end{pmatrix}\cdot\begin{pmatrix} U_{11} & U_{12} & U_{13} & U_{14} \\ U_{21} & U_{22} & U_{23} & U_{24} \\ U_{31} & U_{32} & U_{33} & U_{34} \\ U_{41} & U_{42} & U_{43} & U_{44} \end{pmatrix}
$$

$$
\cdot\begin{pmatrix} d_1^3d_2^3d_3^2d_4 & & & \\ & d_1^3d_2^2d_3^2d_4 & & \\ & & d_1^3d_2^2d_3d_4 & \\ & & & d_1^3d_2^2d_3 \end{pmatrix}
$$

$$
=\begin{pmatrix} d_1^4d_2^3d_3^2d_4U_{11} & d_1^4d_2^2d_3^2d_4U_{12} & d_1^4d_2^2d_3d_4U_{13} & d_1^4d_2^2d_3U_{14} \\ d_1^4d_2^4d_3^2d_4U_{21} & d_1^4d_2^3d_3^2d_4U_{22} & d_1^4d_2^3d_3d_4U_{23} & d_1^4d_2^3d_3U_{24} \\ d_1^4d_2^4d_3^3d_4U_{31} & d_1^4d_2^3d_3^3d_4U_{32} & d_1^4d_2^3d_3^2d_4U_{33} & d_1^4d_2^3d_3^2U_{34} \\ d_1^4d_2^4d_3^3d_4^2U_{41} & d_1^4d_2^3d_3^3d_4^2U_{42} & d_1^4d_2^3d_3^2d_4^2U_{43} & d_1^4d_2^3d_3^2d_4U_{44} \end{pmatrix}
$$

$\equiv 0(\bmod |d_1^4 d_2^3 d_3^2 d_4|)$

显然，$A \cup A_0$的各元素都被$d_1^4 d_2^3 d_3^2 d_4$所整除，即 $A \cup A_0 \equiv 0(\bmod |A|)$ 成立的必要且充分条件是（2）成立。

第十五章　p-adic数

一、提　　要

定义　若

$x = x_0 = a_0 + a_1 p + \cdots + a_{l-2} p^{l-2}$，$0 \leqslant a_\nu < p$是同余式$f(x) \equiv 0 \pmod{p^{l-1}}$的一解且$f'(x_0) \not\equiv 0 \pmod{p}$．则命$x = x_0 + p^{l-1} y$，并研究同余式

$$f(x_0 + p^{l-1} y) \equiv 0 \pmod{p^l},\quad 0 \leqslant y < p$$

即　$f(x_0)/p^{l-1} + f'(x_0) y \equiv 0 \pmod{p}$，$0 \leqslant y < p$ 由此唯一定出y，命它为a_{l-1}，则

$$x = a_0 + a_1 p + \cdots + a_{l-1} p^{l-1},\quad 0 \leqslant a_\nu < p$$

是$f(x) \equiv 0 \pmod{p^l}$的解．此种手续可以无限次地作下去，因此可得－p的幂级数

$$a_0 + a_1 p + \cdots + a_l p^l + \cdots,\quad 0 \leqslant a_\nu < p.$$

以幂级数称为方程$f(x) = 0$的－p-adic解．

定义　形如

$a_0 + a_1 p + \cdots + a_i p^i + \cdots$，$0 \leqslant a_\nu < p$的幂级数，称为$p$-adic数．

一般而言，p-adic数准许有有限多个p的负幂．

定义　命a、b表有理数．对任一有理数有一定有理数值的函数ϕ，若具有以下性质，则称为一赋值：

1）$\phi(a) \geqslant 0$，$\phi(a) = 0$当且仅当$a = 0$；

2）$\phi(ab)=\phi(a)\phi(b)$；

3）$\phi(a+b)\leqslant\phi(a)+\phi(b)$。

定义　如果ϕ满足：

1）$\phi(a)=1$，若$a\neq 0$；

2）$\phi(0)=0$

则称ϕ为恒等赋值。

定义　$\phi(a)=|a|$称为绝对值赋值。

定义　命p表一固定的素数，则任一不等于0的有理数a可唯一地表为

$$a=\frac{r}{s}p^n,\ s>0,\ (r,\ s)=1,\ p\nmid rs,\ 且r、s、n是整数。$$

我们称$\phi(a)=p^{-n}$，$a\neq 0$；$\phi(0)=0$为p-adic赋值，记作

$$\phi(a)=|a|_p.$$

定义　两赋值ϕ及ϕ'间若有以下关系：

$$\phi(a)<\phi(b)与\phi'(a)<\phi'(b)$$

同时成立，则称ϕ与ϕ'等价。

定理 1　设ϕ是一非恒等赋值，则与ϕ等价的赋值为

$$\phi'=\phi^s,\ s>0.$$

定义　若有一正整数$n_0>1$，使$\phi(n_0)>1$，则称ϕ为亚几米德赋值；不然，即对于所有正整数n，总有$\phi(n)\leqslant 1$，则称ϕ为非亚几米德赋值。

定理 2　任一亚几米德赋值必与绝对值赋值等价。

定理 3　设ϕ为一非亚几米德赋值，则有不等式：

1）$\phi(a+b)\leqslant\max(\phi(a),\ \phi(b))$；

且若$\phi(a)\neq\phi(b)$，则有

2）$\phi(a+b)=\max(\phi(a),\ \phi(b))$。

反之，若赋值ϕ适合1），则ϕ为非亚几米德赋值。

定理 4　两个非恒等的非亚几米德赋值ϕ与ϕ'等价的充分

必要条件是：对任一非零有理数a，有$w'(a)=sw(a)$，（$s>0$）。其中

$$w'(a)=-\log\phi'(a),\ w(a)=-\log\phi(a).$$

定理 5　任一非恒等的非亚几米德赋值ϕ必与p-adic赋值$|a|_p$等价。

定义　用$\{a_n\}$代表有理数贯：

$$a_1,\ a_2,\ \cdots,\ a_n,\ \cdots$$

定义　设ϕ为一赋值．如果数贯$\{a_n\}$适合以下条件则称为基贯或ϕ-收敛贯：对任一有理数$\varepsilon>0$，有一正整数N存在，当m、$n>N$时，总有$\phi(a_m-a_n)<\varepsilon$恒成立。

定义　两贯$\{a_n\}$、$\{b_n\}$的和、差、积定义为

$$\{a_n\}\pm\{b_n\}=\{a_n\pm b_n\};$$

$$\{a_n\}\{b_n\}=\{a_nb_n\}.$$

定义　对一数贯$\{a_n\}$，如存在一有理数a适合条件：对任一有理数$\varepsilon>0$，有正整数N存在，当$n>N$时，总有$\phi(a_n-a)<\varepsilon$，则称数贯$\{a_n\}$具有ϕ-极限a，并记为$\phi-\lim\limits_{n\to\infty}a_n=a$。

定义　凡以0为ϕ-极限的贯称为零贯；所有零贯的集合用$\{\overline{0}\}$表示。

定义　若二基贯$\{a_n\}$，$\{b_n\}$的差$\{a_n-b_n\}$是一零贯，则称此两贯同余，用

$$\{a_n\}\equiv\{b_n\}\ (\mathrm{mod}\ \{\overline{0}\})$$

表示。

定义　利用同余关系，可将所有的基贯分类．属于同一类的基贯皆同余，不同类的两基贯决不同余．在每一类中任取一基贯$\{a_n\}$，而用$\{\overline{a_n}\}$代表该类．

定义　所有类所成的系统称为有理数的ϕ-扩张，每一类称为ϕ-扩张中的一个数。

定理 6　如果$\phi(a)=|a|$，则此ϕ-扩张就是实数系统.

定义　如果$\phi(a)=|a|_p$，则称此ϕ-扩张为p-adic数系统.

定义　所有类中包含类$\{\overline{a}\}$（a为有理数），此类中任一基贯都ϕ-收敛于同一有理数a，即以a为ϕ-极限，用$\{\overline{a}\}=a$表示.

定义　用$\{\overline{a_n}\}$表示此类中每一基贯所ϕ-收敛的数，即$\phi-\lim\limits_{n\to\infty}a_n=\{\overline{a_n}\}$.

定理 7　当$\{a_n\}$、$\{a_n{}'\}$同属一类时，则有

$$\phi-\lim_{n\to\infty}a_n=\phi-\lim_{n\to\infty}a_n{}'.$$

定义　$\phi(\{\overline{a_n}\})=\lim\limits_{n-\infty}\phi(a_n)$.

定理 8　若$\{a_n\}\equiv\{a_n'\}\pmod{\{\overline{0}\}}$，则

$$\lim_{n\to\infty}\phi(a_n)=\lim_{n\to\infty}\phi(a_n').$$

定理 9　有理数的ϕ-扩张是完整的，即在ϕ-扩张上再实行ϕ-扩张所得的系统不比ϕ-扩张大.

定义　幂级数

$p^{-m}(a_0+a_1p+\cdots+a_lp^l+\cdots)$，$0\leqslant a_\nu<p$且$m\geqslant 0$，为有理数表示成$p$-adic数的一般形式. 如果在上式中有

$$a_{l+\nu}=a_{l+\nu+t}=a_{l+\nu+2t}=\cdots=a_{l+\nu+nt}=\cdots$$
$$(\nu=1,\ 2,\ \cdots,\ t).$$

此处l和t为固定的整数，$t\geqslant 1$，则称此幂级数是循环的.

定理 10　有理数的p-adic表示法是p的循环幂级数；反之，p的循环幂级数是有理数.

定理 11　若$f(x)$是一整系数多项式，且

$$f(x)\equiv g_0(x)h_0(x)\pmod{p};$$

此处$g_0(x)$、$h_0(x)$为互素的二多项式．则在p-adic数范围内有二多项式

$$g(x)\equiv g_0(x),\ h(x)\equiv h_0(x)\ (\mathrm{mod}\ p)$$

使得 $f(x)=g(x)h(x)$．

二、题　　解

§1 引　　言

习题 1　求出方程$x^2=7$之另一 3 -adic解．

解：由例 2 知道，求方程$x^2=7$的另外一个3 - adic解，是指求出非$x=1+1\cdot3+1\cdot3^2+0\cdot3^3+2\cdot3^4+\cdots$的3 - adic解．

设$f(x)=x^2-7$．由$f(x)\equiv0\ (\mathrm{mod}\ 3)$ 得$x=a_0=2$，且

$$f'(a_0)\not\equiv0(\mathrm{mod}\ 3).$$

命 $$x=a_0+yp=2+3y$$

由 $f(x)=f(2+3y)=(2+3y)^2-7$

$=9y^2+12y-3\equiv0(\mathrm{mod}\ 3^2)$，

$4y-1\equiv0(\mathrm{mod}\ 3)$

得$y=a_1=1$．命

$$x=a_0+a_1p+yp^2=5+9y$$

由 $f(x)=f(5+9y)=(5+9y)^2-7=81y^2+90y+18$

$\equiv0\ (\mathrm{mod}3^3), 10y+2\equiv0\ (\mathrm{mod}\ 3)$

得$y=a_2=1$．

命 $$x=a_0+a_1p+a_2p^2+yp^3=14+3^3y$$

由 $f(x)=f(14+3^3y)=3^6y^2+28\times3^3y+189\equiv0\ (\mathrm{mod}3^4)$，

$28y+7\equiv0\ (\mathrm{mod}\ 3)$

得$y=a_3=2$．

命　　$x = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + y p^4 = 68 + 3^4 y$

由　$f(68+3^4 y) = 3^8 y^2 + 136\times 3^4 y + 4617 \equiv 0 \pmod{3^4}$，

$136y + 57 \equiv 0 \pmod 3$

得$y = a_4 = 0$。

命　　$x = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + a_4 p^4 + y p^5 = 68 + 3^5 y$

由　$f(68+3^5 y) = 3^{10} y^2 + 136\times 3^5 y + 4617 \equiv 0 \pmod{3^6}$

$136y + 19 \equiv 0 \pmod 3$

得$y = a_5 = 2$。

照此方法做下去，可得$x^2 = 7$的另外一个3－adic解

$x = 2 + 1\cdot 3 + 1\cdot 3^2 + 2\cdot 3^3 + 0\cdot 3^4 + 2\cdot 3^5 + \cdots$

因此，方程$x^2 = 7$的两个3－adic解为

$x = 1 + 1\cdot 3 + 1\cdot 3^2 + 0\cdot 3^3 + 2\cdot 3^4 + \cdots$

$x = 2 + 1\cdot 3 + 1\cdot 3^2 + 2\cdot 3^3 + 0\cdot 3^4 + 2\cdot 3^5 + \cdots$

习题 2　求出方程$x^2 + x + 1 = 0$之7－adic解。

解：设$f(x) = x^2 + x + 1$。

由

$$f(x) \equiv 0 \pmod 7$$

得$x = a_0 = 2$，且$f'(a_0) \not\equiv 0 \pmod 7$。

命　　$x = a_0 + yp = 2 + 7y$，

由

$f(2+7y) = 7^2 y^2 + 5\times 7y + 7 \equiv 0 \pmod{7^2}$，

$5y + 1 \equiv 0 \pmod 7$

得$y = a_1 = 4$。

命　　$x = a_0 + a_1 p + y p^2 = 30 + 7^2 y$

由　$f(30+7^2 y) = 7^4 y^2 + 61\times 7^2 y + 931 \equiv 0 \pmod{7^3}$，

$61y + 19 \equiv 0 \pmod 7$

得$y = a_2 = 6$。

命　　$x = a_0 + a_1 p + a_2 p^2 + y p^3 = 324 + 7^3 y$

由 $f(324+7^3y)=7^6y^2+649\times7^3y+105301\equiv0\ (\mathrm{mod}7^4)$,

$$649y+307\equiv0\ (\mathrm{mod}7)$$

得$y=a_3=3$。

命 $x=a_0+a_1p+a_2p^2+a_3p^3+yp^4=1353+7^4y$,

由 $f(1353+7^4y)=7^8y^2+2707\times7^4y+1831963\equiv0\ (\mathrm{mod}7^5)$,

$$2707y+763\equiv0\ (\mathrm{mod}\ 7)$$

得$y=a_4=0$。

继续做下去，可得$x^2+x+1=0$的一个7-adic解：

$$x=2+4\cdot7+6\cdot7^2+3\cdot7^3+0\cdot7^4+\cdots$$

如果由$f(x)\equiv0\ (\mathrm{mod}\ 7)$，取$x=b_0=4$，按照上面使用的方法可得

$$b_1=2,\ b_2=0,\ b_3=3,\ b_4=6,\ \cdots$$

从而可得方程$x^2+x+1=0$的两个7-adic解，它们是：

$$x=2+4\cdot7+6\cdot7^2+3\cdot7^3+0\cdot7^4+\cdots$$

$$x=4+2\cdot7+0\cdot7^2+3\cdot7^3+6\cdot7^4+\cdots.$$

习题3 求出方程$9x^2=7$之3-adic解。

解：设$y=3x$，那么$9x^2=7$变形为$y^2=7$。

由习题1知道，方程$y^2=7$的3-adic解为

$$y=1+1\cdot3+1\cdot3^2+0\cdot3^3+2\cdot3^4+\cdots$$

$$y=2+1\cdot3+1\cdot3^2+2\cdot3^3+0\cdot3^4+2\cdot3^5+\cdots$$

因此，方程$9x^2=7$的3-adic解为

$$x=1\cdot3^{-1}+1\cdot3^0+1\cdot3+0\cdot3^2+2\cdot3^3+\cdots$$

$$x=2\cdot3^{-1}+1\cdot3^0+1\cdot3+2\cdot3^2+0\cdot3^3+2\cdot3^4+\cdots$$

§6 有理数之Φ－扩张

习题1 证明由等价之两赋值所得出的有理数扩张是相同的。

证：设ϕ和ϕ'是两个等价的赋值。不失一般，可设它们非恒等赋值。由定理 1 知道，存在常数$s>0$，使得$\phi'=\phi^s$。

由有理数ϕ-扩张的定义，只需证明如果类$\{\overline{a_n}\}$属于ϕ-扩张，则它一定属于ϕ'-扩张即可；因为同理可证如果类$\{\overline{a_n}\}$在ϕ'-扩张之中，那它一定也在ϕ-扩张之中，从而ϕ-扩张与ϕ'-扩张相同。

对于任给的有理数$\varepsilon>0$，取有理数$\varepsilon_1>0$且$\varepsilon_1\leqslant\varepsilon^{\frac{1}{s}}$因为类$\{\overline{a_n}\}$在$\phi$-扩张中，即贯$\{a_n\}$ ϕ-收敛，故可找到正整数N。当正整数m，n合条件$m>N$，$n>N$时，就有

$$\phi(a_m-a_n)<\varepsilon_1$$

$$\phi^s(a_m-a_n)<\varepsilon$$

此即
$$\phi'(a_m-a_n)<\varepsilon$$

故贯$\{a_n\}$ ϕ'-收敛，也就是说，类$\{\overline{a_n}\}$也在ϕ'-扩张之中。

习题 2　证明在非亚几米德赋值之情况下，$\{a_n\}$收敛之必要且充分条件为$\lim\limits_{n\to\infty}\phi(a_{n+1}-a_n)=0$。

证：先证必要性。如果$\{a_n\}$ ϕ-收敛，即对于任给的有理数$\varepsilon>0$，存在正整数N，则当正整数m、n合条件$m>N$、$n>N$时，就有

$$\phi(a_m-a_n)<\varepsilon$$

恒成立。取$m=n+1$，$n>N$就有

$$\phi(a_{n+1}-a_n)<\varepsilon.$$

此即
$$\lim_{n\to\infty}\phi(a_{n+1}-a_n)=0$$

必要性由此得证。

再证充分性。如果

$$\lim_{n\to\infty}\phi(a_{n+1}-a_n)=0.$$

即对于任给的有理数$\varepsilon>0$，存在正整数N，则当正整数n合条件$n>N$时，就有

$$\phi(a_{n+1}-a_n)<\varepsilon$$

恒成立。因此，如果取正整数m，使得$m>n>N$，就有

$$\phi(a_m-a_{m-1})<\varepsilon$$

$$\phi(a_{m-1}-a_{m-2})<\varepsilon$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\phi(a_{n+1}-a_n)<\varepsilon$$

又因为ϕ为非亚几米德赋值，所以有

$$\begin{aligned}\phi(a_m-a_n)&=\phi((a_m-a_{m-1})+(a_{m-1}-a_{m-2})+\cdots\\&\quad+(a_{n+2}-a_{n+1})+(a_{n+1}-a_n))\\&\leqslant\max\{\phi(a_m-a_{m-1}),\ \cdots,\ \phi(a_{n+1}-a_n)\}\end{aligned}$$

故
$$\phi(a_m-a_n)<\varepsilon$$

此即$\{a_n\}$ ϕ-收敛。充分性由此得证。

第十六章　代数数论介绍

一、提　　要

定义　若θ是一系数为有理数的代数方程

$$f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$$

的根，则称θ为代数数。若$f(x)$不可化且$a_n\neq 0$，则称$n=\partial^0 f$为θ的次数。

定理 1　二代数数的和、差、积、商（除数$\neq 0$）仍为代数数。

定义　若θ是一首项系数为1，其它系数为有理整数的不可化方程的根，则称θ为代数整数。

定理 2　代数整数的和、差、积仍然是代数整数。

定义　若θ及θ^{-1}都是代数整数，则θ称为单位数。

定理 3　θ为单位数的充要条件是θ适合一个首项系数为1，而末首系数为± 1的有理整系数方程。

定义　设F为一由复数所成的集合。若F中至少有两个不同的数，并且F中的任意二数的和、差、积、商（除数$\neq 0$）也在F中，则称F为一数域，简称为域。

定理 4　命θ是一n次代数数，则所有形如

$$a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1},\quad (a_k\text{为有理数})$$

的数成一域，且

$$a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}$$

所表示的数各不相同。

定义 定理4中所得的域，称为在有理数域R上添加θ所得的单扩张，记成$R(\theta)$。

定理5 若$\theta \neq 0$，则$R(\theta)$就是由θ经过加、减、乘、除（除数$\neq 0$）所得数的最大集合。

定理6 若命D经过所有的不等于1的无平方因子的整数，则 $R(\sqrt{D})$ 经过所有的二次域。

定义 用$R(\theta)$表一n次代数数域．记$\theta=\theta^{(1)}$，并命$\theta^{(2)}$，…，$\theta^{(n)}$表示θ所适合的不可化方程的其它$n-1$个根。

定义 设$\alpha=a(\theta)=a_0+a_1\theta+\cdots+a_{n-1}\theta^{n-1}$
命$\alpha=\alpha^{(1)}$。称$\alpha^{(k)}=a(\theta^{(k)})$，$(k=2, 3, \cdots, n)$为$\alpha$的共轭数。又称

$$S(\alpha)=\alpha^{(1)}+\cdots+\alpha^{(n)}$$

$$N(\alpha)=\alpha^{(1)}\cdots\alpha^{(n)}$$

为α的迹和矩。

定义 若在$R(\theta)$中能找到一组数α_1，…α_m，使$R(\theta)$中任何一数都可唯一地表成

$$a_1\alpha_1+\cdots+a_m\alpha_m \quad (a_k\text{为有理数})$$

则称α_1，…，α_m为$R(\theta)$的基底。

定理7 $R(\theta)$的任一基底中所含元素个数相同，且都等于n。

定义 设α_1，…，α_n是$R(\theta)$中任意的n个数，称

$$\Delta(\alpha_1, \cdots, \alpha_n)=\begin{vmatrix} \alpha_1^{(1)} & \cdots\alpha_n^{(1)} \\ \cdots\cdots & \cdots\cdots \\ \alpha_1^{(n)} & \cdots\alpha_n^{(n)} \end{vmatrix}^2$$

为$\alpha_1\cdots$，α_n的判别式。

定理8 判别式有下列诸性质：

1）$\Delta(\alpha_1, \cdots, \alpha_n)$为有理数；特别是，若$\alpha_1$，…$\alpha_n$为代数

整数，则$\Delta(\alpha_1, \cdots, \alpha_n)$为有理整数。

2）若$\alpha_1, \cdots, \alpha_n$及$\beta_1, \cdots, \beta_n$为$R(\theta)$的两组基底，且

$$\alpha_j=\sum_{k=1}^{n} a_{jk}\beta_k \ (1\leqslant j\leqslant n)$$

则 $\Delta(\alpha_1, \cdots, \alpha_n)=|a_{jk}|^2\Delta(\beta_1, \cdots, \beta_n)$。

3）若$\alpha_1, \cdots, \alpha_n$为$R(\theta)$的一组基底，则

$$\Delta(\alpha_1, \cdots, \alpha_n)\neq 0；$$

反过来也是对的。

定义 设$\omega_1, \cdots, \omega_m$为$R(\theta)$中的$m$个整数。若$R(\theta)$中的任一整数都可唯一地表成如下形式

$$a_1\omega_1+\cdots+a_m\omega_m \quad (a_k\text{为有理整数})。$$

则称$\omega_1, \cdots, \omega_m$为$R(\theta)$的一组整底。

定理 9 整底的判别式都相等。

定义 称$R(\theta)$整底的判别式为域的基数，用Δ或$\Delta(R(\theta))$表示。

定理10 基数$\Delta\equiv 0$或$1 \pmod 4$。

定理11 若D为一无平方因子的有理整数。

命

$$\Delta=\begin{cases} D, \\ 4D. \end{cases} ; \quad \omega=\begin{cases} \dfrac{1+\sqrt{D}}{2}, \\ \sqrt{d} \end{cases} , \quad \text{当} \begin{matrix} D\equiv 1 \pmod 4； \\ D\equiv 2, 3 \pmod 4。\end{matrix}$$

则Δ为$R(\sqrt{D})$的基数，而1、ω为一组整底；1、$\dfrac{\Delta+\sqrt{\Delta}}{2}$也为$R(\sqrt{D})$的一组整底。

定义 设α、β为二整数，如果有一整数γ，使$\alpha=\beta\gamma$，则称β可整除α，记成$\beta|\alpha$。

定义 若二整数α、β仅相差一个单位因子，则α与β称为相结

个。

定义 对于整数α，若有$R(\theta)$中的整数β和γ，且均非单位数，使$\alpha=\beta\gamma$，则称α在$R(\theta)$中可分解；否则称为不可分解。

定义 命α_1，…，α_q为$R(\theta)$中的任意q个整数，称所有形如

$$\eta_1\alpha_1+\cdots+\eta_q\alpha_q \quad (\eta_k\text{为}R(\theta)\text{中的整数})$$

的整数所成的集合，为由α_1，…，α_q演成的理想数，用〔α_1,…，α_q〕表示。

定义 由一个整数α所演成的理想数〔α〕，称为主理想数。

定义 理想数〔1〕表示由$R(\theta)$中全体整数所成的集合，称为单位理想数，以O表示。

定义 设$\mathbf{A}=$〔α_1，…，α_q〕及$\mathbf{B}=$〔β_1，…，β_r〕为$R(\theta)$上二理想数。当A中每一整数均B在中，而B中每一整数均在A中时，称它们相等，并记成$\mathbf{A}=\mathbf{B}$。

定义 理想数

〔$\alpha_1\beta_1$，…$\alpha_1\beta_r$，$\alpha_2\beta_1$，…，$\alpha_2\beta_r$，…，$\alpha_q\beta_r$〕

称为理想数

$\mathbf{A}=$〔α_1，…，α_q〕及$\mathbf{B}=$〔β_1，…，β_r〕

的乘积，记成$\mathbf{A}\cdot\mathbf{B}$。

定义 命A及B为二理想数，若有理想数C，使$\mathbf{A}=\mathbf{B}\cdot\mathbf{C}$，则称B整除A，记成$\mathbf{B}|\mathbf{A}$；B、C称为A的因子。

定理12 若$\mathbf{B}|\mathbf{A}$，则A中任一整数都在B中；其逆定理也成立。

定理13 对于任何理想数A，一定能找到一个理想数B，使得$\mathbf{B}\cdot\mathbf{A}=$〔$a$〕，其中$a$为一自然数。

定义 若一理想数除了O及本身以外无别的因子，则称它为素理想数，用P表示。

定理14　任给二理想数

$$A=[\alpha_1,\ \cdots,\ \alpha_q]\ 及B=[\beta_1,\ \cdots,\ \beta_r]$$

则有唯一的理想数D具有下列性质：

1）D|A，D|B；

2）若另有一理想数D_1，D_1|A，D_1|B，则D_1|D。

定理15　$D=[\alpha_1,\ \cdots,\ \alpha_q,\ B_1,\ \cdots\beta_r]$ 就是有上述性质的理想数。

定义　定理14中的D称为A、B的最大公因子，用D=(A, B)表示。一般地可以定义

$$(A_1,\ \cdots,\ A_{m-1},\ A_m)=((A_1,\ \cdots,\ A_{m-1}),\ A_m).$$

若（A，B）=O，则称A、B互素。

定理16　任一不同于O的理想数A都可以分解为素理想数的乘积；如果不计排列顺序，则分解法唯一。

定理17　设A为$R(\theta)$上的任一理想数，则在A中必能找到n个整数

$$\alpha_1=a_{11}\omega_1$$

$$\alpha_2=a_{21}\omega_1+a_{22}\omega_2$$

$$\cdots\cdots$$

$$\alpha_n=a_{n1}\omega_1+a_{n2}\omega_2+\cdots+a_{nn}\omega_n$$

其中a_{ij}都是有理整数，且$a_{ii}>0$（$1\leqslant i\leqslant n$），而$0\leqslant a_{ji}<a_{ii}$（$1\leqslant i<j\leqslant n$），使$\alpha_1$，…，$\alpha_n$成为A的标准基底。

定义　若A|[α]，则称A可以整除α，以A|α表示。

定义　若A|$\alpha-\beta$；α、β为$R(\theta)$中的整数，则称α与β对模A同同，用$\alpha\equiv\beta$(mod A）表示。

定义　根据同余关系，可将$R(\theta)$中的整数进行分类，使凡属于同类的数对模A是互相同余的，而属于不同类的整数不能对模A同余。称这种类为A的剩余类；用$N(A)$表示类数，$N(A)$也称为A的距。

定理18 命Δ为$R(\theta)$的基数，$\Delta(\mathbf{A})$ 为**A**的基底的判别式，则

$$\Delta(\mathbf{A})=(N(\mathbf{A}))^2\Delta.$$

定理19 对于主理想数〔α〕的距$N(〔\alpha〕)$，有

$$N(〔\alpha〕)=|N(\alpha)|.$$

定理20 若**P**为一素理想数，a为任何不能被**P**整除的整数，则

$$a^{N(\mathbf{p})-1}\equiv 1\ (\mathrm{mod}\mathbf{P}).$$

定理21 凡素理想数**P**必整除一个有理素数p，且p为**P**中最小的有理正整数，故是唯一的。

定理22 如果$〔p〕=\mathbf{P}_1\mathbf{P}_2\cdots\mathbf{P}_t$，则

$$p^n=N(〔p〕)=N(\mathbf{P}_1)\cdots N(\mathbf{P}_t).$$

定理23 $\mathbf{P}^2|p$的必要且充分条件是$p|\Delta$。

定理24 在$R(\sqrt{D})$中有一单位数η存在，使凡$R(\sqrt{D})$中的单位数均可表为

$$\pm\eta^n,\quad(n=0,\ \pm1,\ \pm2,\ \cdots)$$

的形式；η称为$R(\sqrt{D})$的基本单位数。

定义 对于二理想数**A**及**B**，若有二主理想数〔α〕及〔β〕，使得

$$〔\alpha〕\mathbf{A}=〔\beta〕\mathbf{B}$$

则称**A**与**B**相似，用**A**～**B**表示。称理想数**A**和**B**属于同一理想数类。

定理25 $R(\theta)$上理想数类的个数有限。

定义 若二理想数**A**与**B**间有如下关系：存在整数α与β，使$〔\alpha〕\mathbf{A}=〔\beta〕\mathbf{B}$且$N(\alpha\beta)>0$，则称**A**与**B**狭义相似，记成$\mathbf{A}\approx\mathbf{B}$。

定义 命A为$R(\sqrt{D})$上的一个理想数，并设α_1、α_2为**A**的一组基底，且适合

$$\alpha_1\alpha_2'-\alpha_1'\alpha_2=N(\mathbf{A})\sqrt{\Delta}$$

此处α_1'、α_2'表α_1、α_2的共轭数。称

$$F(x,y)=\frac{N(\alpha_1x+\alpha_2y)}{N(\mathbf{A})}=\frac{(\alpha_1x+\alpha_2y)(\alpha_1'x+\alpha_2'y)}{N(\mathbf{A})}$$

$$=ax^2+bxy+cy^2$$

为属于**A**的二次型。

定义 若二次型$F(x,y)$属于理想数**A**，则称$F(x,y)$的特征系为理想数**A**的特征系。即若命p_1，…，p_s为Δ的奇素因子，取**A**中整数α，使得

$$\left(\frac{N(\alpha)}{N(\mathbf{A})},\quad 2\Delta\right)=1$$

则称

$$\left(\frac{N(\alpha)/N(\mathbf{A})}{p_i}\right),\quad (i=1,\ 2,\ \cdots,\ s)\ ;$$

$$\delta(\alpha)=(-1)^{\frac{1}{2}\left[\frac{N(\alpha)}{N(\mathbf{A})}-1\right]},\qquad 若D=\frac{\Delta}{4}\equiv 3\ (\bmod 4)；$$

$$\varepsilon(\alpha)=(-1)^{\frac{1}{8}\left[\left(\frac{N(\alpha)}{N(\mathbf{A})}\right)^2-1\right]},\quad 若D=\frac{\Delta}{4}\equiv 2\ (\bmod 8)；$$

$$\delta(\alpha)\varepsilon(\alpha),\qquad 若D=\frac{\Delta}{4}\equiv 6\ (\bmod 8).$$

为理想数**A**的特征系。

定义 两个具有相同特征系的狭义相似类，称为属于同一族。

定理26 每一族中所含的类数（狭义相似类）相等。

定义 命h_0表理想数类（非狭义的）的类数．若$h_0=1$，则称$R(\sqrt{D})$为单域。

定理27 凡单域中整数唯一分解定理成立。

定义 若对$R(\sqrt{D})$中任一数δ，必有整数k，使得

$$|N(\delta-k)|<1$$

则称$R(\sqrt{D})$为欧几里德域。

定理28 凡欧几里德域必为单域。

定理29 仅有五个二次虚欧几里德域：

$R(\sqrt{-1})$，$R(\sqrt{2})$，$R(\sqrt{-3})$，$R(\sqrt{-7})$，

$R(\sqrt{-11})$。

定理30 $R(\sqrt{D})$ 当且仅当$D=2$，3，5，6，7，11，13，17，19，21，29，33，37，41，57，73时为实欧几里德域。

定理31 Mersenne数$M=2^p-1$为素数的必要且充分条件为

$$r_{p-1}\equiv 0\ (\bmod M)\ .$$

其中$r_m=\varepsilon^{2^m}+\varepsilon'^{2^m}$，$\varepsilon$为 $R(\sqrt{D})$ 中的单位数，$N(\varepsilon)=-1$，ε'为ε的共轭数，且$\left(\frac{\Delta}{M}\right)=-1$，$\Delta>0$。

定理32 在$R(\sqrt{-1})$ 中无整数使

$$\xi^4+\eta^4=\tau^2,\ \xi\eta\tau\neq 0\ .$$

定理33 在$R(\rho)$中无整数使

$$\xi^3+\eta^3+\zeta^3=0,\ \xi\eta\zeta\neq 0$$

其中$\rho=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$。

二、题　解

§1　代数数

习题 1　试证系数为代数数的代数方程的根还是代数数。

证： 设ω是方程

$$f(x)=\alpha_0x^n+\alpha_1x^{n-1}+\cdots+\alpha_n=0$$

的根，$f(x)$的系数都是代数数。

如果α_i是有理系数多项式$f_i(x)$ ($i=0, 1, \cdots, n$) 的根，那么α_0，α_1，…，α_n 也是有理系数多项式

$$\Phi(x)=f_0(x)f_1(x)\cdots f_n(x)$$

的根。设$\partial^0\Phi=m$。用β_1，…，β_m表示$\Phi(x)$的所有根。作多项式

$$H(x)=\prod_{i_0,i_1,\cdots,i_n}(\beta_{i_0}x^n+\beta_{i_1}x^{n-1}+\cdots+\beta_{i_n})$$

其中i_0，i_1，…，i_n 的每一个通过值均为 1，2，…，m，而且 i_0，i_1，…，i_n 两两不同。显然，$H(x)$的系数是在有理数域上关于β_1，…β_m的对称函数。根据对称多项式的基本定理，$H(x)$ 的系数全为有理数。又因为

$$f(x)=\alpha_0x^n+\cdots+\alpha_n$$

是$H(x)$的一个因子，所以，ω 是有理系数代数方程 $H(x)=0$ 的根，因此ω是代数数。故系数为代数数的代数方程的根还是代数数。

习题 2　试证首项系数为 1，且有代数整数为系数的代数方程的根还是代数整数。

证： 证法同习题 1，此处只需设ω是方程

$$f(x)=x^n+\alpha_1x^{n-1}+\cdots+\alpha_n=0$$

的根，其中 α_1，…，α_n 是代数整数；α_i是有理整系数多项式 $f_i(x)$ ($i=1$，…，n) 的根，而且

$$\Phi(x)=f_1(x)\cdots f_n(x),\ \partial^\circ\Phi=m.$$

此时，$H(x)$形如

$$H(x)=\prod_{i_1,\ \cdots,\ i_n}(x^n+\beta_{i_1}x^{n-1}+\cdots+\beta_{i_n})$$

显然，$H(x)$是首项系数为 1 且有有理整系数的多项式，而ω是 $H(x)=0$ 的根。因此，ω是一个代数整数。

习题 3 试证以代数整数为系数，且首末项系数皆为单位数的方程之根还是单位数。

证： 设ω是多项式

$$f(x)=\alpha_0x^n+\alpha_1x^{n-1}+\cdots+\alpha_{n-1}x+\alpha_n$$

的根．α_0，α_n 是单位数，α_1，α_2，…，α_{n-1}是代数整数．又设

$$N(\alpha_0)=\alpha_0{}^{(1)}\alpha_0{}^{(2)}\cdots\alpha_0{}^{(l)}$$

$\alpha_0=\alpha_0{}^{(1)}$，而$\alpha_0{}^{(2)}$，…$\alpha_0{}^{(l)}$是$\alpha_0$所适合的首项系数为 1、末项系数为 ±1、次数为l的有理整系数不可化多项式的其它 $l-1$ 个根．由根与系数的关系可得$N(\alpha_0)=\pm1$，因此是ω多项式

$$\frac{N(\alpha_0)}{\alpha_0}f(x)=\pm x^n+\frac{N(\alpha_0)}{\alpha_0}\alpha_1x^{n-1}+\cdots\cdots$$

$$+\frac{N(\alpha_0)}{\alpha_0}\alpha_{n-1}x+\frac{N(\alpha_0)}{\alpha_0}\alpha_n$$

的根．从而，ω是多项式

$$\frac{N(\alpha_0)}{\alpha_0}f(x)=x^n+\frac{N(\alpha_0)}{\alpha_0}\alpha_1x^{n-1}+\cdots\cdots$$

$$+\frac{N(\alpha_0)}{\alpha_0}\alpha_{n-1}x+\frac{N(\alpha_0)}{\alpha_0}\alpha_n \qquad (1)$$

或 $$-\frac{N(\alpha_0)}{\alpha_0}f(x)=x^n-\frac{N(\alpha_0)}{\alpha_0}\alpha_1x^{n-1}-\cdots\cdots$$

$$-\frac{N(\alpha_0)}{\alpha_0}a_{n-1}x-\frac{N(\alpha_0)}{\alpha_0}a_n \qquad (2)$$

的根。显然

$$\frac{N(\alpha_0)}{\alpha_0}\alpha_1,\ \cdots,\ \frac{N(\alpha_0)}{\alpha_0}a_n$$

都是代数整数。由习题 2 知ω是代数整数。

另外，从（1）、（2）可知ω^{-1}是方程

$$1+\frac{N(\alpha_0)}{\alpha_0}a_1x+\cdots+\frac{N(\alpha_0)}{\alpha_0}a_{n-1}x^{n-1}+\frac{N(\alpha_0)}{\alpha_0}a_n x^n$$

$$=0 \qquad (3)$$

或 $$1-\frac{N(\alpha_0)}{\alpha_0}a_1x-\cdots-\frac{N(\alpha_0)}{\alpha_0}a_{n-1}x^{n-1}-\frac{N(\alpha_0)}{\alpha_0}a_n x^n$$

$$=0 \qquad (4)$$

的根。而（3）、（4）左、右两端同时乘上

$$\left[N\left(\frac{N(\alpha_0)}{\alpha_0}\right)\Big/\frac{N(\alpha_0)}{\alpha_0}\right]\cdot a_n^{-1}$$

后，都可化成首项系数为± 1，进而化成首项系数为 1 且有代数整数为系数的代数方程。因此由习题 2 可知ω^{-1}也是代数整数，再据单位数的定义知道ω是单位数。

§7 理想数的唯一分解定理

习题 1 任于二理想数A及B，必有一整数α，使A|[α]，且([α]，AB)＝A。

证： 设A＝[α_1，⋯，α_m]，B＝[β_1，⋯，β_n]

由理想数的乘法和最大公因式的定义知道：

([α]，AB)＝A

即

$[\alpha,\ \alpha_1\beta_1,\ \cdots,\alpha_m\beta_1,\cdots,\ \alpha_1\beta_n\ ,\cdots,\alpha_m\beta_n\ ]=[\alpha_1,\ \cdots,\ \alpha_m]$。

下面对理想数B的生成元个数n行归纳法证明本题。

（一）　当$n=1$时，

$$A=[\alpha_1,\ \cdots,\ \alpha_m],\ B=[\beta_1]$$

对A的生成元个数m行归纳法，以证明$n=1$时结论成立。

i)　当$m=1$时，$A=[\alpha_1]$，$B=[\beta_1]$。若取$\alpha=\alpha_1$，显然有$A|[\alpha]$且$[\alpha,\ \alpha_1\beta_1]=[\alpha_1]$。

ii)　假设结论对于m从2到$t-1$时都成立，则：

对于$A_1=[\alpha_1,\cdots,\ \alpha_{t-2},\ \alpha_{t-1}]$，$B=[\beta_1]$，存在整数$\delta_1$，合条件$A_1|[\delta_1]$，并且

$$[\delta_1,\ \alpha_1\beta_1,\ \cdots,\ \alpha_{t-2}\beta_1,\ \alpha_{t-1}\beta_1]$$
$$=[\alpha_1,\ \cdots,\ \alpha_{t-2},\ \alpha_{t-1}] \qquad (1)$$

对于$A_2=[\alpha_1,\ \cdots,\ \alpha_{t-2},\ \alpha_t]$，$B=[\beta_1]$，存在整数$\delta_2$，合条件$A_2|[\delta_2]$，并且

$$[\delta_2,\ \alpha_1\beta_1,\ \cdots,\ \alpha_{t-2}\beta_1,\ \alpha_t\beta_1]$$
$$=[\alpha_1,\ \cdots,\ \alpha_{t-2},\ \alpha_t] \qquad (2)$$

对于$A_3=[\delta_1,\ \delta_2]$，$B_1=[\alpha_1\beta_1]$，存在整数$\alpha$，合条件$A_3|[\alpha]$，并且

$$[\alpha,\ \delta_1(\alpha_1\beta_1),\ \delta_2(\alpha_1\beta_1)]=[\delta_1,\ \delta_2] \qquad (3)$$

再由（1）、（2）有

$$[\delta_1,\ \delta_2,\ \delta_1\beta_1,\ \cdots,\ \alpha_t\beta_1]=[\alpha_1,\ \cdots,\ \alpha_t] \qquad (4)$$

把（3）代入（4）得

$$[\alpha,\ \alpha_1\beta_1,\ \cdots,\alpha_t\beta_1]=[\alpha_1,\ \cdots,\alpha_t]$$

此即结论对于$m=t$时也成立。从而$n=1$时本题结论成立。

（二）　归纳假定$n=k-1$时，本题结论成立．即对于

$$A=[\alpha_1,\ \cdots,\ \alpha_m],\ B=[\beta_1,\ \cdots,\ \beta_{k-1}]$$

存在整数α，合条件$\mathbf{A}|[\alpha]$，并且有

$$[\alpha,\ \alpha_1\beta_1,\ \cdots,\ \alpha_m\beta_1,\ \cdots,\ \alpha_1\beta_{k-1},\ \cdots,\ \alpha_m\beta_{k-1}]$$
$$=[\alpha_1,\ \cdots,\ \alpha_m] \qquad (5)$$

由（5）有

$$([\alpha,\ \alpha_1\beta_1,\ \cdots\alpha_m\beta_1,\ \cdots,\ \alpha_1\beta_{k-1},\ \cdots,\ \alpha_m\beta_{k-1}],[\alpha_1\beta_k,\ \cdots,\ \alpha_m\beta_k])=([\alpha_1,\ \cdots,\ \alpha_m],\ [\alpha_1\beta_k,\ \cdots\alpha_m\beta_k])$$

此即

$$[\alpha,\ \alpha_1\beta_1,\ \cdots,\alpha_m\beta_1,\cdots,\alpha_1\beta_k,\ \cdots,\alpha_m\beta_k]=[\alpha_1,\cdots,\ \alpha_m].$$

故$n=k$时本题结论也成立。由（一）、（二）可知，本题结论正确。

习题 2　任何理想数$\mathbf{A}$皆能表为$[\alpha,\ \beta]$的形式，α、β皆为整数，且β可取为$\mathbf{A}$中任何整数。

证：设$\mathbf{A}=[q_1,\ \cdots,\ q_m]$

对$\mathbf{A}$中任何一个整数β，可取$\mathbf{B}$，使得

$$\mathbf{AB}=[\beta].$$

由习题1可知，存在整数α，合条件$\mathbf{A}|[\alpha]$，并且有

$$([\alpha],\mathbf{AB})=\mathbf{A}$$
$$([\alpha],\ [\beta])=\mathbf{A}$$

即
$$[\alpha,\ \beta]=\mathbf{A}.$$

§8　理想数的基底

习题　令$\omega_1,\ \cdots,\ \omega_n$为$R(\theta)$的一组整底，则$\alpha_i\omega_j$（$1\leqslant i\leqslant n,\ 1\leqslant j\leqslant n$）能唯一地表成

$$x_1\alpha_1+\cdots+x_n\alpha_n\quad(x_i\text{全为有理整数})$$

之形式乃$\alpha_1,\ \cdots,\ \alpha_n$为某理想的基底的充分必要条件。

证：先证必要性。设$\alpha_1,\ \cdots,\ \alpha_n$是理想数$\mathbf{A}=[q_1,\ \cdots,\ q_m]$的基底，那么对于$\alpha_i$，存在整数$\eta_l\in R(\theta)$，使得

$$\alpha_i = \eta_1 q_1 + \cdots + \eta_m q_m$$

因此 $$\alpha_i\omega_j = (\eta_1\omega)q_1 + \cdots + (\eta_m\omega_j)q_m$$

从而 $\alpha_i\omega_j \in \mathbf{A}$。又因为$\alpha_1$，…，$\alpha_m$是$\mathbf{A}$的基底，故存在有理整数$x_1$，…，$x_n$，使$\alpha_i\omega_j$可唯一地表成

$$\alpha_i\omega_j = x_1\alpha_1 + \cdots + x_n\alpha_n\ .$$

再证充分性。习题中“某理想数”表明，我们只需证明合题设条件的α_1，…，α_n是某一个具体理想数的基底即可。下面证明α_1，…，α_n是$\mathbf{A}=[\alpha_1, \cdots, \alpha_n]$的基底。

i) α_1，…，α_n是$\mathbf{A}_i=[\alpha_i]$（$1\leqslant i\leqslant n$）的基底。

对于任一整数$q\in\mathbf{A}_i$，存在整数$\delta\in R(\theta)$，使得

$$q=\delta\alpha_i \tag{1}$$

又因为ω_1，…，ω_n是$R(\theta)$的一组整底，故有有理整数y_l，使δ唯一地表成

$$\delta = y_1\omega_1 + \cdots + y_n\omega_n \tag{2}$$

把（2）代入（1）得

$$q = y_1(\alpha_i\omega_1) + \cdots + y_n(\alpha_i\omega_n) \tag{3}$$

再由已知，存在有理整数x_{ll}'，使$\alpha_i\omega_j$可唯一地表成

$$\begin{aligned} \alpha_i\omega_1 &= x_{11}\alpha_1 + \cdots + x_{1n}\alpha_n \\ \alpha_i\omega_2 &= x_{21}\alpha_1 + \cdots + x_{2n}\alpha_n \\ &\cdots\cdots \\ \alpha_i\omega_n &= x_{n1}\alpha_1 + \cdots + x_{nn}\alpha_n \end{aligned} \tag{4}$$

把（4）代入（3）得

$$q = y_1'\alpha_1 + \cdots + y_l'\alpha_n$$

其中 $y_l' = y_1x_{1l} + y_2x_{2l} + \cdots + y_nx_{nl}$（$1\leqslant l\leqslant n$）显然$y_l'$是有理整数，故$\alpha_1$，…，$\alpha_n$是理想数$\mathbf{A}=[\alpha_i]$（$1\leqslant i\leqslant n$）的基底。

ii) α_1，…，α_n是理想数$\mathbf{A}=[\alpha_1, \cdots, \alpha_n]$的基底。对于任一整数$Q\in\mathbf{A}$，存在整数$\delta_l\in R(\theta)$使得

$$Q=\delta_1\alpha_1+\cdots+\delta_n\alpha_n \qquad (5)$$

又因为$\delta_i\alpha_i\in[\alpha_i]$（$1\leqslant i\leqslant n$）；由i)知$\alpha_1$，…，$\alpha_n$是$[\alpha_1]$，…，$[\alpha_n]$的基底，故存在有理整数$X_{ll'}$，使得

$$\begin{aligned}
\delta_1\alpha_1 &= X_{11}\alpha_1+\cdots+X_{1n}\alpha_n\\
\delta_2\alpha_2 &= X_{21}\alpha_1+\cdots+X_{2n}\alpha_n\\
&\cdots\cdots \qquad (6)\\
\delta_n\alpha_n &= X_{n1}\alpha_1+\cdots+X_{nn}\alpha_n
\end{aligned}$$

把（6）代入（5）得

$$Q=X_1\alpha_1+\cdots+X_n\alpha_n$$

其中 $X_l=X_{1l}+X_{2l}+\cdots+X_{nl}$（$1\leqslant l\leqslant n$）

显然X_l是有理整数，故α_1，…，α_n是理想数$\mathbf{A}=[\alpha_1, \cdots, \alpha_n]$的基底。充分性由此得证。

说明：下面的结论并不真实

设α_1，…，$\alpha_n\in\mathbf{A}$，则$\alpha_i\omega_j$能唯一地表成

$$x_1\alpha_1+\cdots+x_n\alpha_n$$

的形式是α_1，…，α_n为$\mathbf{A}$的基底的充要条件。

请看一个例子：取$\theta=i$，$R(\theta)$的一组整底是$\omega_1=1$，$\omega_2=i$；取$\mathbf{A}=[1]$；$\alpha_1=a$，$\alpha_2=ai$，a为有理整数且$a\neq\pm1$．显然α_1，$\alpha_2\in\mathbf{A}$，并且$\alpha_i\omega_j$（$1\leqslant i\leqslant 2$，$1\leqslant j\leqslant 2$）可唯一地表示成

$$\begin{aligned}
\alpha_1\omega_1 &= 1\cdot\alpha_1+0\cdot\alpha_2\\
\alpha_2\omega_1 &= 0\cdot\alpha_1+1\cdot\alpha_2\\
\alpha_1\omega_2 &= 0\cdot\alpha_1+1\cdot\alpha_2\\
\alpha_2\omega_2 &= -1\cdot\alpha_1+0\cdot\alpha_2
\end{aligned}$$

但$\alpha_1=a$、$\alpha_2=ai$不是$\mathbf{A}=[1]$的基底。

§10 素理想数

习题 设$\theta=\sqrt[3]{pq^2}$，$\bar{\theta}=\sqrt[3]{p^2q}$，其中$p$、$q$为有理素数，且

满足下述条件：

$p\equiv 1\pmod 3$；$q\not\equiv 2,\ 3$；$pq^2\not\equiv 1\pmod 9$；

$q^{\frac{p-1}{3}}\not\equiv 1\pmod p$．

求证：

1） $R(\theta)=R(\bar\theta)$为一三次域；

2） 1、θ、$\bar\theta$为$R(\theta)$的一组整底；

3） $R(\theta)$中没有整数ω，使

$$1,\ \omega,\ \omega^2$$

成为$R(\theta)$的整底；

4） 试在$R(\theta)$中分解下列理想数：

$$[2],\ [3],\ [p],\ [q].$$

证：1） $R(\theta)=R(\bar\theta)$为一三次域。

$\theta,\bar\theta$分别适合的方程

$$x^3-pq^2=0\ 和\ x^3-p^2q=0$$

显然都不可化。又对于任意的$\alpha\in R(\theta)$，都有有理数a_0、a_1、a_2，使得

$$\alpha=a_0+a_1\theta+a_2\theta^2$$

取$b_0=a_0$，$b_1=a_2q$，$b_2=\frac{a_1}{p}$，上式就变为

$$\alpha=b_0+b_1\bar\theta+b_2\bar\theta^2$$

此即$\alpha\in R(\bar\theta)$.同理可证对于任意的$\beta\in R(\bar\theta)$，也会有$\beta\in R(\theta)$，故 $R(\theta)=R(\bar\theta)$为一三次域。

2） 1、θ、$\bar\theta$为$R(\theta)$的一组整底．下面用反证法证明．如果1、θ、$\bar\theta$不是$R(\theta)$的一组整底，就一定有整数$\alpha\in R(\theta)$，

$$\alpha=a_0+a_1\theta+a_2\bar\theta$$

其中a_0、a_1、a_2不全是有理整数．不失一般，设a_1非有理整数，

且设$a_1=\frac{m}{n}$、m、n均为有理整数，$(m, n)=1$，$n>1$．再由$\bar{\theta}=\frac{1}{q}\theta^2$，就有

$$\begin{cases} a=a^{(1)}=a_0+\frac{m}{n}\theta^{(1)}+\frac{a_2}{q}\theta^{(1)^2} \\ a^{(2)}=a_0+\frac{m}{n}\theta^{(2)}+\frac{a_2}{q}\theta^{(2)^2} \\ a^{(3)}=a_0+\frac{m}{n}\theta(3)+\frac{a_2}{q}\theta^{(3)^2} \end{cases} \quad (1)$$

把$\theta^{(1)}=\theta$、$\theta^{(2)}=p\theta$、$\theta^{(3)}=\rho^2\theta$、$\rho=\frac{-1+\sqrt{3}i}{2}$代入（1）得

$$\begin{cases} a^{(1)}=a_0+\frac{m}{n}\theta+\frac{a_2}{q}\theta^2 \\ a^{(2)}=a_0+\frac{m}{n}\rho\theta+\frac{a_2}{q}\rho^2\theta^2 \\ a^{(3)}=a_0+\frac{m}{n}\rho^2\theta+\frac{a_2}{p}\rho\theta^2 \end{cases} \quad (2)$$

设 $F(x)=\prod_{i=1}^{3}(x-a^{(i)})$

由（2）有

$$F(x)=x^3-3a_0x^2+(3a_0{}^2-3\cdot\frac{m}{n}a_2pq)x-\left[a_0{}^3+\left(\left(\frac{m}{n}\right)^3\cdot q-3a_0\left(\frac{m}{n}\right)a_2\right)pq+a_2{}^3p^2q\right]$$

因此a是方程

$n^3x^3-3n^3a_0x^2+(3n^3a_0{}^2-3n^2ma_2pq)x-[n^3a_0{}^3+(m^3q-$

$3n^2a_0ma_2)pq+n^3a_2{}^3q^2q]=0$ （3）

的根。由于α是整数，（3）给出在$R(\theta)$内

$$n^2|pq^2m^3$$

因而可找到整数$\delta_1\in R(\theta)$，使得

$$pq^2m^3=\delta_1n^2$$

$$N(pq^2m^3)=N(\delta_1n^2)$$

$$p^3q^6m^9=N(\delta_1)n^6$$

再由$(m, n)=1$且$n>1$可得$n=q$。把$n==q$代入（3）得

$$q^3x^3-3q^3a_0x^2+(3q^3a_0{}^2-3q^3ma_2p)x-[q^3a_0{}^3+(m^3q$$

$$-3q^2a_0ma_2)pq+q^4a_2{}^3p^2]=0 \quad (4)$$

由（4）知道在$R(\theta)$内

$$q^3|m^3pq^2,\ q|m^3p$$

因此又存在整数$\delta_2\in R(\theta)$，使得

$$m^3p=\delta_2q$$

$$N(m^3p)=N(\delta_2q)$$

$$m^9p^3=N(\delta_2)q^3$$

又由$(m, q)=1$，就有$q=p$。再据已知条件$p\equiv1\ (\mathrm{mod}\ 3)$可推出$pq^2\equiv p^3\equiv1\ (\mathrm{mod}\ 9)$，此与$pq^2\not\equiv1\ (\mathrm{mod}\ 9)$相矛盾。故1、$\theta$、$\bar\theta$一定是$R(\theta)$的一组整底。

3） $R(\theta)$中没有整数ω，使1、ω、ω^2是$R(\theta)$的整底。

命ω为$R(\theta)$中任一整数，则有有理整数a、b、c，使得

$$\omega=a+b\theta+c\bar\theta$$

由于 $\theta\bar\theta=pq$，$\theta^2=q\bar\theta$，$\bar\theta^2=p\theta$

因此 $\omega^2=(a+b\theta+c\bar\theta)^2=(a^2+2bcpq)+(c^2p+2ab)\theta+(b^2q+2ac)\bar\theta$

$$\Delta(1,\omega,\omega^2)=\begin{vmatrix}1 & a & a^2+2bcpq\\ 0 & b & c^2p+2ab\\ 0 & c & b^2q+2ac\end{vmatrix}^2\Delta(1,\theta,\bar\theta)=$$

$$=(b^3q-c^3p)^2\cdot\Delta$$

i) 如果$b^3q=c^3p$, $\Delta(1,\ \omega,\ \omega^2)=0$，1、$\omega$、$\omega^2$非整底。

ii) 如果$b^3q=c^3p+1$, $b^3q\equiv1(\mathrm{mod}\,p)$; $(b^3q)^{\frac{p-1}{8}}\equiv1$ (mod$p$)；又因为 $b^{p-1}\equiv1(\mathrm{mod}\,p)$故$q^{\frac{p-1}{8}}\equiv1(\mathrm{mod}\,p)$，与$q^{\frac{p-1}{8}}\not\equiv1$ (mod$p$) 相矛盾。

iii) 如果$b^3q=c^3p-1$, $b^3q\equiv-1\,(\mathrm{mod}\,p)$，因$\frac{p-1}{8}$为偶数，也有$q^{\frac{p-1}{8}}\equiv1\,(\mathrm{mod}\,p)$，仍然与$q^{\frac{p-1}{8}}\not\equiv1\,(\mathrm{mod}\,p)$矛盾。

从i)、ii)、iii) 可知

$$b^3q-c^3p\neq0;\ b^3q-c^3p\neq\pm1$$

因此

$$\Delta(1,\ \omega,\ \omega^2)\equiv0\ (\mathrm{mod}\,\Delta)$$

且
$$|\Delta(1,\ \omega,\ \omega^2)|>|\Delta|.$$

故 1、ω, ω^2不是$R(\theta)$的一组整底。

4) 在$R(\theta)$中分解下列理想数：

〔2〕，〔3〕，〔p〕，〔q〕。

先算出$R(\theta)$的基数Δ

$$\Delta=\Delta(1,\ \theta,\ \bar\theta)=\begin{vmatrix}1 & \theta^{(1)} & \bar\theta^{(1)}\\ 1 & \theta^{(2)} & \bar\theta^{(2)}\\ 1 & \theta^{(3)} & \bar\theta^{(3)}\end{vmatrix}^2$$

$$=\begin{vmatrix}1 & \theta^{(1)} & \frac{1}{q}\theta^{(1)^2}\\ 1 & \theta^{(2)} & \frac{1}{q}\theta^{(2)^2}\\ 1 & \theta^{(3)} & \frac{1}{q}\theta^{(3)^2}\end{vmatrix}^2=$$

$$=\frac{1}{q^2}\begin{vmatrix}1 & \theta & \theta^2\\ 1 & \rho\theta & \rho^2\theta^2\\ 1 & \rho^2\theta & \rho\theta^2\end{vmatrix}^2=\frac{\theta^6}{q^2}\begin{vmatrix}1 & 1 & 1\\ 1 & \rho & \rho^2\\ 1 & \rho^2 & \rho\end{vmatrix}$$

$$=\frac{\left(p^{\frac{1}{3}}q^{\frac{2}{3}}\right)^6}{q^2}(-27)=-27p^2q^2$$

以**P**、**Q**、**R**表$R(\theta)$上的素理想数，**O**表单位理想数．首先证明〔2〕是$R(\theta)$上的一个素理想数。

在$R(\theta)$上，〔2〕的分解式为下列五种形式之一：

i)　〔2〕$=\mathbf{PQR}$，**P**、**Q**、**R**各不相同，而$N(\mathbf{P})=N(\mathbf{Q})$ $=N(\mathbf{R})=2$；

ii)　〔2〕$=\mathbf{P}^2\mathbf{Q}$，$\mathbf{P}\neq\mathbf{Q}$，而$N(\mathbf{P})=N(\mathbf{Q})=2$；

iii)　〔2〕$=\mathbf{P}^3$，$N(\mathbf{P})=2$；

Ⅳ)　〔2〕$=\mathbf{PQ}$，$N(\mathbf{P})=2$而$N(\mathbf{Q})=2^2$；

Ⅴ)　〔2〕$=\mathbf{P}$，$N(\mathbf{P})=2^3$．

对于前四种情形，〔2〕都有距为2的素因子**P**，因此首先研究这种情形．设

$$a_0,\ b_0+b_1\theta,\ c_0+c_1\theta+c_2\bar{\theta}$$

为**P**的一组标准基底，则

$$b_0<a_0,\ c_0<a_0,\ c_1<b_1.$$

又因$a_0\theta$，$a_0\bar{\theta}$均在**P**中，所以又有$b_1\leqslant a_0$，$c_2\leqslant a_0$．于是，由$N(\mathbf{P})=a_0b_1c_2=2$得

$a_0=2$，$b_1=c_2=1$，$c_1=0$，$b_0=0$或1，$c_0=0$或1

因此**P**必为如下四种形式之一：

〔$2,\ \theta,\ \bar{\theta}$〕；〔$2,\ \theta,\ 1+\bar{\theta}$〕；

〔$2,\ 1+\theta,\ \bar{\theta}$〕；〔$2,\ 1+\theta,\ 1+\bar{\theta}$〕．

显然$\mathbf{P}\neq$〔$2,\theta,\bar{\theta}$〕，否则$\theta\cdot\bar{\theta}=pq$也在**P**中．而$(pq,\ 2)=1$，于是$\mathbf{P}=\mathbf{O}$．同理可证$\mathbf{P}\neq$〔$2,\ \theta,\ 1+\bar{\theta}$〕，$\mathbf{P}\neq$〔$2,\ 1+\theta,$

$\bar{\theta}$〕. 因此〔2〕在i）～Ⅳ）的分解形式中只可能是第iii）种形式，即

$$〔2〕=〔2,\ 1+\theta,\ 1+\bar{\theta}〕^3=\mathbf{P}^3.$$

上式给出$\mathbf{P}^3 | 2$，$\mathbf{P}^2 | 2$.

另外，由Dedekind判别式定理：$\mathbf{P}^2 | p_1$的充要条件是$p_1 | \Delta$. 这里$p_1=2$，$\Delta=-27p^2q^2$，$p\equiv 1\pmod 3$，$q\neq 2$，故

$$〔2〕\neq\mathbf{P}^3.$$

故〔2〕的分解形式不是i）～Ⅳ）四种形式，而只能是第Ⅳ）种形式. 也就是说，〔2〕是$R(\theta)$上的素理想数.

再证明〔3〕在$R(\theta)$上的分解式为

〔3〕=〔3，$2+\theta$，$2+\bar{\theta}$〕^{3}，当$q\equiv 1\pmod 3$时；

〔3〕=〔3，$2+\theta$，$1+\bar{\theta}$〕^{3}，当$q\equiv 2\pmod 3$时.

〔3〕在$R(\theta)$上的分解式只能是下列五种形式之一：

i）〔3〕=**PQR**，**P**、**Q**、**R**各不相同，而$N(\mathbf{P})=N(\mathbf{Q})=N(\mathbf{R})=3$；

ii）〔3〕=$\mathbf{P}^2\mathbf{Q}$，$\mathbf{P}\neq\mathbf{Q}$而$N(\mathbf{P})=N(\mathbf{Q})=3$；

iii）〔3〕=$\mathbf{P}^3$，$N(\mathbf{P})=3$；

Ⅳ）〔3〕=**PQ**，$N(\mathbf{P})=3$，$N(\mathbf{Q})=3^2$；

Ⅴ）〔3〕=**P**，$N(\mathbf{P})=3^3$.

前四种情形，〔3〕都有距为3的素因子**P**. 先研究此种情形. 设

$$a_0,\ b_0+b_1\theta,\ c_0+c_1\theta+c_2\bar{\theta}$$

为**P**的一组标准基底，则

$$b_0<a_0,\ c_0<a_0,\ c_1<b_1$$

又因$a_0\theta$、$a_0\bar{\theta}$均在**P**中，因此$b_1\leqslant a_0$，$c_2\leqslant a_0$. 由

$$N(\mathbf{P})=a_0b_1c_2=3$$

可得 $a_0=3$，$b_1=c_2=1$，$c_1=0$，$b_0=0$或1或2，$c_0=0$或1或2.

因此P可能为下面九种形式之一：

$[3, \theta, \bar{\theta}]$；$[3, 1+\theta, \bar{\theta}]$；$[3, 2+\theta, \bar{\theta}]$；

$[3, \theta, 1+\bar{\theta}]$；$[3, 1+\theta, 1+\bar{\theta}]$；$[3, 2+\theta, 1+\bar{\theta}]$；

$[3, \theta, 2+\bar{\theta}]$；$[3, 1+\theta, 2+\bar{\theta}]$；$[3, 2+\theta, 2+\bar{\theta}]$。

$P \neq [3, \theta, \bar{\theta}]$，否则$\theta\bar{\theta} = pq$也在P中，而$(pq, 3) = 1$，从而$P = O$，此与P为素理想数矛盾。同理可证

$$P \neq [3, \theta, 1+\bar{\theta}]$$

$$P \neq [3, \theta, 2+\bar{\theta}]$$

$$P \neq [3, 1+\theta, \bar{\theta}]$$

$P \neq [3, 1+\theta, 1+\bar{\theta}]$，其理由为

$$3, 1+\theta, 1+\bar{\theta}$$

不能是基底，否则由

$$(1+\bar{\theta})\bar{\theta} = 3x_1 + x_2(1+\theta) + x_3(1+\bar{\theta})$$

有
$$x_1 = -\frac{p+1}{3}$$

其中x_1、x_2、x_3都是有理整数，因此$3 \mid p+1$，此与题设$p \equiv 1 \pmod 3$相矛盾；

$P \neq [3, 1+\theta, 2+\bar{\theta}]$，否则由

$$(2+\bar{\theta})\bar{\theta} = 3x_1 + x_2(1+\theta) + x_3(2+\bar{\theta}) \text{ 得}$$

$$x_1 = -\frac{p+4}{3}$$

也与$p \equiv 1 \pmod 3$矛盾；

$P \neq [3, 2+\theta, \bar{\theta}]$，否则由

$$(2+\theta)\theta = 3x_1 + x_2(2+\theta) + x_3\bar{\theta}$$

得
$$3x_1 + 4 = 0$$

此也不可能。

因此，P只可能是如下两种形式之一：

$$[3,\ 2+\theta,\ 1+\bar{\theta}];\ [3,\ 2+\theta,\ 2+\bar{\theta}].$$

当$q\equiv 1 \pmod 3$时．$P\neq[3,\ 2+\theta,\ 1+\bar{\theta}]$，否则

$$\theta(1+\bar{\theta})-(2+\theta)=pq-2$$

也在P中，而$(pq-2,\ 3)=1$，从而$P=O$，此不可能。

另一方面：

$$(2+\theta)\theta=-\frac{2q+4}{3}\cdot 3+2(2+\theta)+q(2+\bar{\theta})$$

$$(2+\theta)\bar{\theta}=\frac{pq-4}{3}\cdot 3+2(2+\bar{\theta})$$

$$(2+\bar{\theta})\bar{\theta}=-\frac{2p+4}{3}\cdot 3+p(2+\theta)+2(2+\bar{\theta})$$

$$(2+\bar{\theta})\theta=\frac{pq-4}{3}\cdot 3+2(2+\theta)$$

因此　　　$3,\ 2+\theta,\ 2+\bar{\theta}$

的确是素理想数P的一组标准基底．再由Dedekind判别式定理可知，$q\equiv 1 \pmod 3$时

$$[3]=[3,\ 2+\theta,\ 2+\bar{\theta}]^3$$

当$q\equiv 2 \pmod 3$时，$P\neq[3,\ 2+\theta,\ 2+\bar{\theta}]$，否则

$$\bar{\theta}(2+\theta)-2(2+\bar{\theta})=pq-4$$

也在P中．而$(pq-4,\ 3)=1$，从而$P=O$，此不可能。

另一方面：

$$(2+\theta)\theta=-\frac{q+4}{3}\cdot 3+2(2+\theta)+q(1+\bar{\theta})$$

$$(2+\theta)\bar{\theta}=\frac{pq-2}{3}\cdot 3+2(1+\bar{\theta})$$

$$(1+\bar{\theta})\bar{\theta}=-\frac{2p+1}{3}\cdot 3+p(2+\theta)+(1+\bar{\theta})$$

$$(1+\bar{\theta})\theta=\frac{pq-2}{3}\cdot 3+(2+\theta)$$

因此 $3,\ 2+\theta,\ 1+\bar{\theta}$

的确是素理想数**P**的一组标准基底，再由 Dedekind 判别式定理可知当$q\equiv 2\ (\text{mod}\ 3)$ 时

$$[3]=[3,\ 2+\theta,\ 1+\bar{\theta}]^3.$$

综上所述，〔3〕在$R(\theta)$上的分解式为：

$$[3]=\begin{cases}[3,\ 2+\theta,\ 2+\bar{\theta}]^2, & \text{当}q\equiv 1\ (\text{mod}\ 3)\ \text{时；}\\ [3,\ 2+\theta,\ 1+\bar{\theta}]^3, & \text{当}q\equiv 2\ (\text{mod}\ 3)\ \text{时.}\end{cases}$$

最后证明〔q〕，〔q〕在$R(\theta)$上的分解式为

$$[p]=[p,\ \theta,\ \bar{\theta}]^3$$
$$[q]=[q,\ \theta,\ \bar{\theta}]^3$$

〔p〕在$R(\theta)$上的分解式只能是下列五种形式之一：

i) 〔p〕$=\mathbf{PQR}$，**P**、**Q**、**R**各不相同，而且 $N(\mathbf{P})=N(\mathbf{Q})=N(\mathbf{R})=p$；

ii) 〔p〕$=\mathbf{P}^2\mathbf{Q}$，$\mathbf{P}\neq\mathbf{Q}$，$N(\mathbf{P})=N(\mathbf{Q})=p$；

iii) 〔p〕$=\mathbf{P}^3$，$N(\mathbf{P})=p$；

Ⅳ) 〔p〕$=\mathbf{PQ}$，$N(\mathbf{P})=p$，$N(\mathbf{Q})=p^2$；

Ⅴ) 〔p〕$=\mathbf{P}$，$N(\mathbf{P})=p^3$.

前四种形式，〔p〕都有距为p的素因子**P**，因此先研究这种情形．设

$$a_0,\ b_0+b_1\theta,\ c_0+c_1\theta+c_2\bar{\theta}$$

为**P**的一组标准基底，则

$$b_0<a_0,\ c_0<a_0,\ c_1<b_1.$$

又因$a_0\theta$，$a_0\bar{\theta}$ 均在**P**中，故有

$$b_1\leqslant a_0,\ c_2\leqslant a_0.$$

由 $$N(\mathbf{P})=a_0b_1c_2=p$$

可得$a_0=p$，$b_1=c_2=1$，$c_1=0$，b_0、c_0取0，1，…，$p-1$诸数中的一数．因此，**P**为下面p^2种形式之一：

$$[p,\ a+\theta,\ b+\bar{\theta}],\quad 0\leqslant a\leqslant p-1,\quad 0\leqslant b\leqslant p-1.$$

因为$a+\theta$、$b+\bar{\theta}$均在**P**中，即有

$$\mathbf{P}|[a+\theta],\ \mathbf{P}|[b+\bar{\theta}].$$

因此在$R(\theta)$上可找到二理想数$\mathbf{A}_1$、$\mathbf{A}_2$，使得

$$[a+\theta]=\mathbf{PA}_1,\quad [b+\bar{\theta}]=\mathbf{PA}_2;$$

$$N(a+\theta)=N(\mathbf{P})N(\mathbf{A}_1),N(b+\bar{\theta})=N(\mathbf{P})N(\mathbf{A}_2).$$

又因为$N(\mathbf{P})=p$且$N(\mathbf{P}_1)$，$N(\mathbf{P}_2)$均为有理整数，故有

$$N(a+\theta)\equiv 0\ (\mathrm{mod}p)$$

$$N(b+\bar{\theta})\equiv 0\ (\mathrm{mod}p)$$

再由θ、$\bar{\theta}$分别是方程

$$x^3=pq^2\text{和}x^3=p^2q$$

的根知道$a+\theta$、$b+\bar{\theta}$分别是方程

$$(x-a)^3=pq^2\text{和}\ (x-b)^3=p^2q$$

的根．由根与系数的关系就有

$$N(a+\theta)=a^3+pq^2$$

$$N(b+\bar{\theta})=b^3+p^2q$$

故a、b适合三次同余式：

$$a^3+pq^2\equiv 0\,(\mathrm{mod}p)$$

$$b^3+p^2q\equiv 0\,(\mathrm{mod}p)$$

因为$0\leqslant a\leqslant p-1$，$0\leqslant b\leqslant p-1$，因此上面两个同余式给出$a=b=0$，从而

$$\mathbf{P}=[p,\ \theta,\ \bar{\theta}].$$

另一方面：

$$\theta\cdot\theta=q\bar{\theta}$$

$$\theta\cdot\bar{\theta}=pq$$

$$\bar{\theta}\cdot\bar{\theta}=p\theta$$

因此 $p, \theta, \bar{\theta}$

的确是P的一组标准基底．再由Dedekind判别式定理可得

$$[p]=[p, \theta, \bar{\theta}]^3$$

用完全相同的方法可得

$$[q]=[q, \theta, \bar{\theta}]^3.$$

故$[p]$，$[q]$在$R(\theta)$上的分解式为

$$[p]=[p, \bar{\theta}, \theta]^3$$

$$[q]=[q, \theta, \bar{\theta}]^3.$$

§11 单位数

习题 试证若基本单位数$\eta=X+Y\sqrt{D}$的系数为有理整数，则X、Y为

$$u^2-v^2D=N(\eta)$$

的最小正整数解．若X、Y不是有理整数，则$\eta^3=u+v\sqrt{D}$的系数u、v即为上式的最小正整数解．

证：i） 如果X、Y为有理整数．设

$$u_0+v_0\sqrt{D}$$

是不定方程

$$u^2-v^2D=N(\eta)$$

的基本解，则存在整数m，使得

$$X+Y\sqrt{D}=(u_0+v_0\sqrt{D})^m \qquad (1)$$

又因$\eta=X+Y\sqrt{D}$是基本单位数，故也可找到整数n，使得

$$u_0+v_0\sqrt{D}=(X+Y\sqrt{D})^n \qquad (2)$$

把（2）代入（1）得

$$X+Y\sqrt{D}=(X+Y\sqrt{D})^{mn}$$

从而$m=n=1$或$m=n=-1$．但是$m=-1$给出$Y=-v_0<0$，此

与$X+Y\sqrt{D}$为 $R(\sqrt{D})$ 上的基本单位数$X>0$、$Y>0$ 相矛盾，故$m=1$。

此时有 $$X+Y\sqrt{D}=u_0+v_0\sqrt{D}$$

所以X、Y为 $$u^2-v^2D=N(\eta)$$

的最小正整数解。

ii) 如果X、Y非有理整数，由二次域$R(\sqrt{D})$的基本性质有

$$X=\frac{a}{2},\quad Y=\frac{b}{2},\quad a>0,\quad b>0,$$

$$a\equiv b\equiv 1\ (\mathrm{mod}\,2),\quad D\equiv 1\ (\mathrm{mod}\,4).$$

由 $$D\equiv 1\ (\mathrm{mod}\,4)$$

得 $$D\equiv 1,\ 5\ (\mathrm{mod}\,3)$$

再由 $$N(\eta)=\left(\frac{a}{2}+\frac{b}{2}\sqrt{D}\right)\left(\frac{a}{2}-\frac{b}{2}\sqrt{D}\right)$$

$$=\frac{a^2}{4}-\frac{b^2}{4}D$$

和 $$a^2-b^2D=4N(\eta)$$

得 $$D\equiv 5\ (\mathrm{mod}\,8)$$

因若 $$D\equiv 1\ (\mathrm{mod}\,8)$$

$$a^2\equiv b^2\equiv 1\ (\mathrm{mod}\,8),\quad N(\eta)=\pm 1,\quad a^2-b^2D=4N(\eta)$$

就会给出

$$0\equiv\pm 4\ (\mathrm{mod}\,8)$$

此不可能。另一方面

$$\eta^2=\frac{a^2+b^2D}{4}+\frac{ab}{2}\sqrt{D}$$

其中 $$\frac{a^2+b^2D}{4}\text{和}\frac{ab}{2}$$

均非有理整数。

$$\eta^3=\frac{a(a^2+3b^2D)}{8}+\frac{b(3a^2+b^2D)}{8}\sqrt{D}$$

其中 $\frac{a(a^2+3b^2D)}{8}$ 和 $\frac{b(3a^2+b^2D)}{8}$

均为有理整数，并且显然有

$$\eta^3<\eta^4<\cdots<\eta^n<\cdots$$

故η^3的系数为不定方程$u^2-v^2D=N(\eta)$的最小正整数解。

§4 族

习题1 当$\Delta>0$，而基本单位数适合$N(\eta)=+1$时，试求理想数$[\sqrt{\Delta}]$的特征系。

解：设p_1，…，p_s为Δ的奇素数因子，$\alpha=\sqrt{\Delta}$，$\mathbf{A}=[\alpha]$。显然$\alpha\in\mathbf{A}$。又从

$$N(\alpha)=\sqrt{\Delta}(-\sqrt{\Delta})=-\Delta,\quad N(\mathbf{A})=\Delta$$

可得 $$\left(\frac{N(\alpha)}{N(\mathbf{A})},\ 2\Delta\right)=(-1,\ 2\Delta)=1$$

故理想数$\mathbf{A}=[\sqrt{\Delta}]$的特征系为：

$$\left(\frac{N(\alpha)/N(\mathbf{A})}{p_i}\right)=\left(\frac{-1}{p_i}\right)=(-1)^{\frac{p_i-1}{2}},\quad 1\leqslant i\leqslant s$$

及 $$\delta(\alpha)=(-1)^{\frac{1}{2}\left[\frac{N(\alpha)}{N(\mathbf{A})}-1\right]}=-1,$$

$$\text{若}D=\frac{\Delta}{4}\equiv 3\pmod 4;$$

$$\varepsilon(\alpha)=(-1)^{\frac{1}{8}\left[\left(\frac{N(\alpha)}{N(\mathbf{A})}\right)^2-1\right]}=1,$$

若 $\frac{\Delta}{4}\equiv 2(\mathrm{mod}8)$；

$$\delta(\alpha)\varepsilon(\alpha)=-1, \qquad 若 \ \frac{\Delta}{4}\equiv 6(\mathrm{mod}8).$$

习题 2 若理想数**A**的特征系与**B**或**B**$[\sqrt{\Delta}]$的特征系相同，则称**A**与**B**属于同一族（广义的）．试证在这样的定义之下，若**A**$\sim$**B**，则**A**、**B**必属于同一族，且每一族中所含的类数相同．

证：先证如果**A**$\sim$**B**，则**A**、**B**必属于同一族（广义的）．因为狭义相似类的特征系全同，故只需证明如果**A**$\sim$**B**，就一定有**A**$\approx$**B**或**A**$\approx$**B**$[\sqrt{\Delta}]$即可．

因为**A**$\sim$**B**，故有整数α、$\beta\in R(\sqrt{D})$，使得

$$[\alpha]\mathbf{A}=[\beta]\mathbf{B}.$$

i) 如果$\Delta<0$．设

$$\alpha\beta=\frac{a+b\sqrt{D}}{2}, \quad a、b为有理整数$$

且 $a\equiv b(\mathrm{mod}\,2)$， 当$D\equiv 1\,(\mathrm{mod}7)$ 时；

$a\equiv b\equiv 0\,(\mathrm{mod}\,2)$，当$D\equiv 2, 3\,(\mathrm{mod}\,4)$ 时；

$$\Delta=\begin{cases} D, & 当D\equiv 1\,(\mathrm{mod}\,4)\ 时; \\ 4D, & 当D\equiv 2,\ 3\,(\mathrm{mod}\,4)\ 时. \end{cases}$$

因为$\Delta<0$，从而

$$D<0, \quad N(\alpha\beta)=\frac{a^2-b^2D}{4}>0$$

故 $$\mathbf{A}\approx\mathbf{B}.$$

讨论： 如果$N(\eta)=-1$，因为

$$[\eta][\sqrt{\Delta}]=[\sqrt{\Delta}]=[\sqrt{\Delta}][1]$$

且 $N(\eta\sqrt{\Delta})=\Delta>0$，

故 $[\sqrt{\Delta}]\approx[1]$，

即$[\sqrt{\Delta}]$属于主类，此种情形$[\sqrt{\Delta}]$的特征值全部为1．

ii) 如果$\Delta>0$而基本单位数η适合$N(\eta)=-1$．则因

$$[\alpha]\mathbf{A}=[\beta]\mathbf{B}=[\eta\beta]\mathbf{A}$$

并且$N(\alpha\beta)$与$N(\alpha\beta\eta)$中必有一为正，故此种情形也有

$$\mathbf{A}\approx\mathbf{B}.$$

iii) 如果$\Delta>0$，而基本单位数η适合$N(\eta)=1$

则当$N(\alpha\beta)>0$时，就有$\mathbf{A}\approx\mathbf{B}$；

当$N(\alpha\beta)<0$时，由$[\alpha]\mathbf{A}=[\beta]\mathbf{B}$可得

$$[\alpha\sqrt{\Delta}]\mathbf{A}=[\beta]\mathbf{B}[\sqrt{\Delta}]$$

且因 $N(\alpha\sqrt{\Delta}\beta)=N(\sqrt{\Delta})N(\alpha\beta)=-\Delta N(\alpha\beta)>0$

故此时就有 $\mathbf{A}\approx\mathbf{B}[\sqrt{\Delta}]$.

再证每一族（广义的）中所含的类数相同．

我们称$\mathbf{A}$、$\mathbf{B}$属于同一类，当且仅当$\mathbf{A}\approx\mathbf{B}$或者$\mathbf{A}\approx\mathbf{B}[\sqrt{\Delta}]$．照此定义，把$R(\sqrt{D})$中的理想数分成$h$类：

$$\{\mathbf{A}_1\},\ \{\mathbf{A}_2\},\ \cdots\{\mathbf{A}_h\}$$

不失一般，可设类$\{\mathbf{A}_1\}$，…，$\{\mathbf{A}_i\}$的特征值合条件：理想数$\mathbf{A}_j$或者$\mathbf{A}_j[\sqrt{\Delta}]$的特征值全为1，$1\leqslant j\leqslant i$．用$\mathbf{I}$表示主族，显然

$$\mathbf{I}=\{\{\mathbf{A}_1\},\{\mathbf{A}_2\},\ \cdots,\ \{\mathbf{A}_i\}\}$$

再用$\mathbf{I}\{\mathbf{A}\}$表$\mathbf{I}$中各类与$\{\mathbf{A}\}$乘积类的集合，即

$$\mathbf{I}\{\mathbf{A}\}=\{\{\mathbf{A}\mathbf{A}_1\},\ \{\mathbf{A}\mathbf{A}_2\},\ \cdots,\ \{\mathbf{A}\mathbf{A}_i\}\}.$$

若将理想数类分成若干集合：

$$\mathbf{I},\ \mathbf{I}\{\mathbf{A}'_{i+1}\},\ \mathbf{I}\{\mathbf{A}'_{i+2}\},\ \cdots,\ \mathbf{I}\{\mathbf{A}'_h\} \qquad (1)$$

其中$\{\mathbf{A}'_k\}$不在$\mathbf{I}$，$\mathbf{I}\{\mathbf{A}'_{i+1}\}$，…，$\mathbf{I}\{\mathbf{A}'_{k-1}\}$之中，而

$$\mathbf{A}'_{i+1},\ \cdots,\mathbf{A}'_h$$

是 $$\mathbf{A}_{i+1},\ \cdots,\ \mathbf{A}_h$$

的一个全排列．易见必无理想数类同时属于（1）中二个不同的集合．因若不然，可设

$$\{\mathbf{A}\}\in\mathbf{I}\{\mathbf{A}'_{i+1}\}$$

$$\{A\}\in I\{A'_{i+2}\}$$

从而找到类$\{A_0\}$，$\{B_0\}\in I$，使得

$$\{A\}=\{A_0\}\{A'_{i+1}\}$$

$$\{A\}=\{B_0\}\{A'_{i+2}\}$$

从而 $$\{A_0\}\{A'_{i+1}\}=\{B_0\}\{A'_{i+2}\} \quad (2)$$

设类$\{B_0\}$的逆类为$\{R_0\}$，即

$$R_0B_0=[a]，a\text{为自然数。}$$

（2）式两边同乘$\{R_0\}$，得

$$\{R_0A_0\}\{A'_{i+1}\}=\{[a]\}\{A'_{i+2}\} \quad (3)$$

又因为 $\{[a]\}=\{[1]\}$

代入（3）式得 $$\{R_0A_0\}\{A'_{i+1}\}=\{A'_{i+2}\} \quad (4)$$

再由$\{R_0A_0\}\in I$，（4）式就给出

$$\{A'_{i+2}\}\in I\{A'_{i+1}\}$$

与假设矛盾。

另一方面，理想数AB的特征系中各值即为A、B的对应特征值的乘积。又因为$\{A'_r\}(i+1\leqslant r\leqslant h)$中任意两个理想数$A'_r$、$A''_r$合条件$A'_r\approx A''_r$或$A'_r\approx A''_r[\sqrt{\Delta}]$，而狭义相似类的特征系又是全同的，因此$A'_r$的特征系与$A''_r$或$A''_r[\sqrt{\Delta}]$的特征系相同。所以（1）中任一集合内的各类都在同一族中。又从前证知道，无理想数类同时属于（1）中二个不同的集合，从而（1）中不同的集合属于不同的族，因此（1）中每一集合即为一族。再因为$I\{A'_r\}(i+1\leqslant r\leqslant h)$中任何二类都不相同（从$I\{A\}$的定义立得），故$I\{A'_r\}(i+1\leqslant r\leqslant h)$中所含理想数类的类数与I中所含理想数类的类数均为$i$，此即每族中所含类数相同。

第十七章　代数数与超越数

一、提　　要

定义　一实数可以看成直线上一点，一组实数称为一个点集。

定义　如果两个点集之间可以建立一一对应关系，则称它们为同幂。

同幂关系有如下三性质：

i)　A与A同幂；

ii)　若A与B同幂，则B与A同幂；

iii)　若A与B，B与C同幂，则A与C同幂。

定义　与自然数集同幂的点集称为无限可数集；无限可数集与有限集都称为可数集。

定理 1　可数个可数集的并集是可数集。

定理 2　有理数集是可数集。

定理 3　（0，1）中的全体实数成一不可数集。

定理 4　全体代数数成一可数集。

定义　非代数数的数称为超越数。

定理 5　有超越数存在。

定理 6　任一n次实代数数不能有n级以上的有理渐近分数，即若ξ是一n次代数数，则对任一$\delta>0$及$A>0$，适合不等式

$$|\xi-\frac{p}{q}|<\frac{A}{q^{n+\delta}}$$

的有理整数解（p，q）的对数有限。

定理 7 设$n\geqslant 3$及

$$f(x, y)=b_0x^n+b_1x^{n-1}y+\cdots+b_ny^n$$

为一不可化齐次多项式，其系数为有理整数。

又设 $$g(x,y)=\sum_{r+s\leqslant n-3}g_{rs}x^ry^s$$

为一次数至多是$n-3$的有理乘数多项式。则不定方程

$$f(x、y)=g(x、y)$$

至多有有限对整数解(x,y)。

定理 8 设$n\geqslant 3$及

$$g(x,y)=b_0x^n+b_1x^{n-1}y+\cdots+b_ny^n$$

为一有理整系数不可化齐次多项式，a为有理整数，则

$$g(x、y)=a$$

至多有有限多组整数解。

定理 9 设$n\geqslant 3$，$b^2-4ac\neq 0$，$ad\neq 0$，则不定方程

$$ay^2+by+c=dx^n$$

仅有有限个解。

定理10 设$n\geqslant 3$及

$$f(z)=a_nz^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0$$

是一个整系数的n次不可约（有理数域上）多项式，则不定方程

$$H(x、y)=a_nx^n+a_{n-1}x^{n-1}y+\cdots+a_1xy^{n-1}+a_0y^n=c$$

仅有有限多组整数解x、y。其中c是给定的整数。

定理11 e是超越数。

定理12 π是超越数。

定理13 e^π是超越数。

定理14　如果α是代数数，$\alpha\neq 0$，1，β是一个非有理的代数数，则α^{β}是超越数。

定理15　任给m个不同的代数数

$$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_m$$

则数

$$e^{\alpha_1},\ e^{\alpha_2},\ \cdots,\ e^{\alpha_m}$$

在全体代数数所成的域上线性无关。

定理16　设α_1，…，α_n是任给的n个（$n\geqslant 2$）非零代数数。如果

$$\log\alpha_1,\ \cdots,\ \log\alpha_n$$

在有理数域上线性无关，则

$$1,\ \log\alpha_1,\ \cdots,\ \log\alpha_n$$

在全体代数数所成的域上也是线性无关的。

二、题　　解

§1　超越数之存在定理

习题1　求出定理2之证明中$\frac{a}{b}((a,\ b)=1)$之地位。

解：定理2的证明方法，主要是将0与1之间的既约分数先依分母大小，再依分子大小排列成如下形式：

$$\frac{0}{1},\ \frac{1}{1},\ \frac{1}{2},\ \frac{1}{3},\ \frac{2}{3},\ \frac{1}{4},\ \frac{3}{4},\ \frac{1}{5},\ \frac{2}{5},\ \frac{3}{5},\ \frac{4}{5},\ \cdots\quad(1)$$

并且断言（1）成一无穷可数集合。

下面将证明此点，即证明数列（1）与自然数集合N等幂。从而我们可以说：0与1之间的有理数的个数与全体有理数的个数“一样多”。

用$Q_{[0,1]}$表示数列（1）所成的集合．作函数

$$f: Q_{[0,1]} \longrightarrow N$$

如下图中箭头所指方向，只是有些数要去掉，如$\frac{1}{2}$，$\frac{2}{4}$，$\frac{4}{8}$等均表同一数$\frac{1}{2}$．这样我们的f只对第一个出现的$\frac{1}{2}$有定义，并且$f\left(\frac{1}{2}\right)=3$，不再定义$f\left(\frac{2}{4}\right)$、$f\left(\frac{4}{8}\right)$了．

0 ↘	1	2	3	4	5	6……
1	↘ $\frac{1}{1}$ ↓					
2	$\frac{1}{2}$ ↓					
3	$\frac{1}{3}$ →	$\frac{2}{3}$ ↙				
4	$\frac{1}{4}$ →	$\frac{2}{4}$ →	$\frac{3}{4}$ ↙			
5	$\frac{1}{5}$ →	$\frac{2}{5}$ →	$\frac{3}{5}$ →	$\frac{4}{5}$ ↙		
6	$\frac{1}{6}$ →	$\frac{2}{6}$ →	$\frac{3}{6}$ →	$\frac{4}{6}$ →	$\frac{5}{6}$	
⋮	·	·	·	·	·	·

按照这一规则，我们举例如下：

$$f(0)=1,\quad f\left(\frac{3}{4}\right)=7,$$

$$f\left(\frac{1}{1}\right)=2,\quad f\left(\frac{1}{5}\right)=8,$$

$$f\left(\frac{1}{2}\right)=3,\quad f\left(\frac{2}{5}\right)=9,$$

$$f\left(\frac{1}{3}\right)=4,\quad f\left(\frac{3}{5}\right)=10,$$

$$f\left(\frac{2}{3}\right)=5,\quad f\left(\frac{4}{5}\right)=11,$$

$$f\left(\frac{1}{4}\right)=6,\quad \cdots\cdots$$

显然，上述定义的函数f：$Q_{[0,\ 1]}\longrightarrow N$是一个双射函数，这样就证明了$Q_{[0,\ 1]}$与$N$等幂，再由定理 1 知有理数集$Q$也是无穷可数集，因此，$Q_{[0,\ 1]}$与$Q$等幂．于是可以说：0 与 1 之间的有理数的个数与全体有理数的个数“一样多”．

习题 2　证明可数集之分集为可数集。

证：i)　如果A为有限可数集，那么它的任一分集A^*也是有限集，从而是可数集．

ii)　如果A为无限可数集，则A中所有元素可排列成无穷序列：

$$a_1, a_2, a_3, \cdots, a_n, \cdots$$

如果A^*是A的一个有限子集，由定义就知A^*是可数集。

如果A^*是A的一个无限子集，则所有属于A^*的a的下标作成全体自然数所成集合N的一个无穷子集N^*。由于N的任何无穷子集都可按其元素的大小排成一个无穷序列，因此N^*是可数集合，而N^*与A^*成 1 － 1 对应，所以A^*也是可数集合。

§2　Liouville定理及超越数例子

习题　作出一不可数集，其中每一数都是超越数。

解：作集合

$$A=\left\{\xi \mid \xi=\sum_{m=1}^{\infty}\frac{1}{10^{[a_m]m!}},\quad \begin{array}{l} a_i\text{是正实数并且} \\ 1\leqslant[a_1]<[a_2]<\cdots \end{array}\right\}$$

由实数集合不可数，可以知道集合A也是一个不可数集合。下面再证明A中每一个元素都是超越数。

命 $$\alpha_n=\frac{1}{10^{[a_1]\cdot 1!}}+\frac{1}{10^{[a_2]\cdot 2!}}+\cdots+\frac{1}{10^{[a_n]\cdot n!}}=\frac{p}{q}$$

$$q=10^{[a_n]\cdot n!}\ .$$

则 $$0<\xi-\frac{p}{q}=\frac{1}{10^{[a_{n+1}](n+1)!}}+\frac{1}{10^{[a_{n+2}](n+2)!}}+\cdots$$

$$<\frac{1}{10^{[a_{n+1}](n+1)!}}+\frac{1}{10^{[a_{n+1}](n+2)!}}+\cdots$$

$$<\frac{1}{10^{[a_{n+1}](n+1)!}}\left(1+\frac{1}{10}+\frac{1}{10^2}+\cdots\right)$$

$$=\frac{\frac{10}{9}}{10^{[a_{n+1}](n+1)!}}$$

$$<\frac{\frac{10}{9}}{10^{[a_n](n+1)!}}=\frac{\frac{10}{9}}{q^{n+1}}.$$

此n可以任意，故由提要中定理 6 可知ξ不是代数数．此即A中所有元素都是超越数，故A就是合题设条件的一个集合．

§5 Thue定理之应用

习题 1 设n为一奇数>1．依次排列自然数之平方及n次方：

$$1=z_1<z_2<z_3<\cdots$$

证明 $$z_{\nu+1}-z_\nu\to\infty.$$

证：如果$z_{\nu+1}-z_\nu\to\infty$不真， 那么就一定存在一个正整数M,使得有无穷多个z_ν满足

$$z_{\nu+1}-z_\nu<M$$

从而至少有一个正整数$k<M$，使得

$$z_{\nu+1}-z_\nu=k$$

有无穷多组解，即是在下列诸方程

$$x^2-y^2=k \quad (1)$$

$$x^n-y^n=k \quad (2)$$

$$x^2-y^n=k \quad (3)$$

$$x^n-y^2=k \quad (4)$$

之中，至少有一个具有无穷多组解。

由于$x+y\leqslant k$只能有有限组正整数解，因此方程（1)只有有限组正整数解。

由于 $x^{n-1}+x^{n-2}y+\cdots+xy^{n-2}+y^{n-1}\leqslant k$

只有有限组正整数解，因此方程（2）也只有有限组正整数解；

再从提要中定理9知道，方程（3）、（4）只能有有限组正整数解。

这些就与方程（1）～(4)中至少有一个有无穷多组正整数解相矛盾．故有

$$z_{\nu+1}-z_\nu\to\infty.$$

习题 2 命$\langle\xi\rangle=\min(\xi-[\xi],\ [\xi]+1-\xi)$，且$n$为奇数$>1$，则

$$\lim_{\substack{x\to\infty\\ x\text{非平方数}}} x^{\frac{n}{2}}\langle x^{\frac{n}{2}}\rangle=\infty.$$

证：如果$x^{\frac{n}{2}}\langle x^{\frac{n}{2}}\rangle\to\infty$不真，则一定存在正整数$M$，使得有无穷多个$x$满足

$$x^{\frac{n}{2}}\langle x^{\frac{n}{2}}\rangle<M.$$

i) 当 $\langle x^{\frac{n}{2}}\rangle=x^{\frac{n}{2}}-[x^{\frac{n}{2}}]=\{x^{\frac{n}{2}}\}$时，如果

$$x^{\frac{n}{2}}\langle x^{\frac{n}{2}}\rangle\to\infty$$

不真，则存在无穷多个x，使得

$$x^{\frac{n}{2}}\{x^{\frac{n}{2}}\}<M \qquad (1)$$

更有
$$[x^{\frac{n}{2}}]\{x^{\frac{n}{2}}\}<M. \qquad (2)$$

由（1）有 $x^{\frac{n}{2}}(x^{\frac{n}{2}}-[x^{\frac{n}{2}}])<M$

$$x^n-x^{\frac{n}{2}}[x^{\frac{n}{2}}]<M$$

$$x^n-([x^{\frac{n}{2}}]+\{x^{\frac{n}{2}}\})[x^{\frac{n}{2}}]<M$$

$$x^n-[x^{\frac{n}{2}}]^2<\{x^{\frac{n}{2}}\}[x^{\frac{n}{2}}]+M \qquad (3)$$

把（2）代入（3）得

$$x^n-[x^{\frac{n}{2}}]^2<2M$$

又因为$x^n-[x^{\frac{n}{2}}]^2>0$，因此由上式可知，至少存在一个正整数$k<2M$，使方程

$$x^n-[x^{\frac{n}{2}}]^2=k$$

有无穷多个正整数解。由定理9知此不可能。

ii) 当 $\langle x^{\frac{n}{2}}\rangle=[x^{\frac{n}{2}}]+1-x^{\frac{n}{2}}$时，如果

$$x^{\frac{n}{2}}\langle x^{\frac{n}{2}}\rangle\to\infty$$

不真，则有无穷多个x满足

$$x^{\frac{n}{2}}\langle x^{\frac{n}{2}}\rangle<M$$

$$x^{\frac{n}{2}}([x^{\frac{n}{2}}]+1-x^{\frac{n}{2}})<M$$

$$x^{\frac{n}{2}}([x^{\frac{n}{2}}]+1)<x^n+M$$

$$x^n([x^{\frac{n}{2}}]+1)^2<(x^n+M)^2$$

$$x^n([x^{\frac{n}{2}}]^2+2[x^{\frac{n}{2}}]+1)<x^{2n}+2x^nM+M^2$$

$$[x^{\frac{n}{2}}]^2+2[x^{\frac{n}{2}}]+1<x^n+2M+\frac{M^2}{x^n}$$

因此当x充分大时有

$$[x^{\frac{n}{2}}]^2+2[x^{\frac{n}{2}}]+1-x^n<2M+1 \qquad (4)$$

又因为$[x^{\frac{n}{2}}]^2+2[x^{\frac{n}{2}}]+1-x^n$

$$=(x^{\frac{n}{2}}-\{x^{\frac{n}{2}}\})^2+2(x^{\frac{n}{2}}-\{x^{\frac{n}{2}}\})+1-x^n$$

$$>(x^{\frac{n}{2}}-1)^2+2(x^{\frac{n}{2}}-1)+1-x^n$$

$$=x^n-2x^{\frac{n}{2}}+1+2x^{\frac{n}{2}}-2+1-x^n=0$$

所以由（4）式可知，至少存在一个正整数$k_1<2M+1$，使方程

$$[x^{\frac{n}{2}}]^2+2[x^{\frac{n}{2}}]+1-x^n=k_1$$

即 $$[x^{\frac{n}{2}}]^2+2[x^{\frac{n}{2}}]+(1-k_1)=x^n$$

有无穷多个正整数解，此仍与定理9矛盾。

由i)、ii) 可知

$$\lim_{\substack{x\to\infty \\ x\text{非平方数}}} x^{\frac{n}{2}}\langle x^{\frac{n}{2}}\rangle=\infty$$

说明：本题中没有条件“n为奇数$\geqslant 1$”，显然有误．因若n为偶数，则

$$\langle x^{\frac{n}{2}}\rangle=0,\ \lim_{\substack{x\to\infty \\ x\text{非平方数}}} x^{\frac{n}{2}}\langle x^{\frac{n}{2}}\rangle=0\neq\infty$$

所以n必为奇数；另外，作为Thue定理的应用练习，就应与习题1一样加此条件．

§7 π之超越性

习题1 若ξ是非零有理数，则$\sinh\xi$是超越数。

证：不失一般，可设

$$\xi=\frac{b}{a},\quad (a,\ b)=1,\ a>0,\ b>0$$

此时
$$\sinh\xi=\frac{e^{\xi}-e^{-\xi}}{2}$$

变为
$$\sinh\frac{b}{a}=\frac{e^{\frac{b}{a}}-e^{-\frac{b}{a}}}{2}$$

故只需要证明
$$e^{\frac{b}{a}}-e^{-\frac{b}{a}}$$
为超越数便可。

$e^{\frac{b}{a}}$为超越数。否则可设$e^{\frac{b}{a}}$适合有理系数方程

$$a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$$

即有

$$a_n\left(e^{\frac{b}{a}}\right)^n+a_{n-1}\left(e^{\frac{b}{a}}\right)^{n-1}+\cdots+a_1\left(e^{\frac{b}{a}}\right)+a_0=0$$

$$a_n\left(e^{\frac{1}{a}}\right)^{bn}+a_{n-1}\left(e^{\frac{1}{a}}\right)^{b(n-1)}+\cdots+a_1\left(e^{\frac{1}{a}}\right)^{b}+a_0=0$$

因此 $e^{\frac{1}{a}}$也是代数数，进而

$$\left(e^{\frac{1}{a}}\right)^{a}=e$$

也是代数数。此不可能，故 $e^{\frac{b}{a}}$是超越数。

如果

$$e^{\frac{b}{a}}-e^{-\frac{b}{a}}=\alpha$$

是代数数。又因为

$$e^{\frac{b}{a}}\left(-e^{-\frac{b}{a}}\right)=-1$$

故由根与系数的关系知道 $e^{\frac{b}{a}}$是方程

$$x^2-\alpha x-1=0$$

的根，再由16章第1节习题1知 $e^{\frac{b}{a}}$是代数数，此与前证$e^{\frac{b}{a}}$是超越数相矛盾。因此

$$e^{\frac{b}{a}}-e^{-\frac{b}{a}}$$

是超越数。

说明：原题中的条件“ξ是有理数”显然应改为“ξ是非零有理数”．因为当$\xi=0$时，

$$\sinh\xi=\sinh 0=\frac{e^0-e^{-0}}{2}=0$$

是代数数．

习题2　证明e^i是超越数。因之证明sin 1是超越数。

证：此处证明e^i是超越数所用的方法，与本书证明e是超越数所用的方法（§6 Th_2，Th_3）相同，即只需把多项式$f(x)$的系

数推广到复数域，把整除定义从有理整数推广到Gauss整环上就可以了，

引理　命

$$f(x)=\sum_{m=0}^{n} a_m x^m,\ a_m(0\leqslant m\leqslant n)\text{是复数，}$$

$$F(x)=\sum_{k=0}^{n} f^{(k)}(x),\ F(0)e^x-F(x)=Q(x),$$

则
$$|Q(x)|\leqslant e^{|x|}\sum_{m=0}^{n}|a_m|\,|x|^m$$

证：有恒等式

$$F(x)=\sum_{k=0}^{n}\sum_{m=k}^{n} a_m\frac{m!}{(m-k)!}x^{m-k}$$

$$=\sum_{m=0}^{n} a_m\sum_{k=0}^{m}\frac{m!}{(m-k)!}x^{m-k}$$

$$=\sum_{m=0}^{n} a_m\sum_{k=0}^{m}\frac{m!}{k!}x^{k}$$

特别，有
$$F(0)=\sum_{m=0}^{n} a_m m!\ .$$

故
$$|Q(x)|=\left|\sum_{m=0}^{n} a_m\sum_{k=0}^{\infty}\frac{m!}{k!}x^k-\sum_{m=0}^{n} a\ \sum_{k=0}^{m}\frac{m!}{k!}x^k\right|$$

$$=\left|\sum_{m=0}^{n} a_m\sum_{k=m+1}^{\infty}\frac{m!}{k!}x^k\right|$$

$$\leqslant\sum_{m=0}^{n}|a_m|\sum_{k=m+1}^{\infty}|x|^k\Big/(k-m)!$$

$$=\sum_{m=0}^{n}|a_m||x|^m\sum_{l=1}^{\infty}\frac{|x|^l}{l!}\leqslant e^{|x|}\sum_{m=0}^{n}|a_m||x|^m$$

下面证明e^i是超越数.使用反证法.假定e^i适合$P(x)=0$，而

$$P(x)=\sum_{h=0}^{m}g_hx^h,\quad g_0\neq 0,\quad m>0$$

此处g_h是有理数整．命有理素数p合条件

$$p>\max(m,\ |g_0|)$$

又命
$$f(x)=\frac{x^{p-1}\prod_{h=1}^{m}(ih-x)^p}{(p-1)!}=\sum_{k=0}^{n}a_kx^k \tag{1}$$

此处a_k是复数且$a_k=a_k(p)$.

由于ih是$f(x)=0$的p重根，故可写为

$$f(x)=\frac{(i^m m!)^p x^{p-1}+Apx^p+\cdots}{(p-1)!}$$

$$=\frac{B_{p,h}(x-ih)^p+B_{p+1,h}(x-ih)^{p+1}+\cdots}{(p-1)!}$$

此处A、B都为Gauss整数．由此$f(x)$做出引理中的$F(x)$及$Q(x)$，则

$$0=F(0)P(e^i)=F(0)\sum_{h=0}^{m}g_he^{ih}$$

$$=\sum_{h=0}^{m}g_hF(ih)+\sum_{h=0}^{m}g_hQ(ih) \tag{2}$$

又已知

$$\sum_{h=0}^{m} g_h F(ih) = g_0 \sum_{k=0}^{n} f^{(k)}(0) + \sum_{h=1}^{m} g_h \sum_{k=0}^{n} f^{(k)}(ih)$$

$$= g_0((i^m m!)^p + pAp + \cdots) + \sum_{h=1}^{m} g_h(pBp,h + p(p+1)Bp+1,h + \cdots)$$

此为一Gauss整数．上式右边

$$p \nmid g_0(i^m m!)^p$$

而其余各项都是p的倍数，故有

$$\left|\sum_{h=0}^{m} g_h F(ih)\right| \geqslant 1$$

否则

$$\left|\sum_{h=0}^{m} g_h F(ih)\right| = 0$$

$$\sum_{h=0}^{m} g_h F(ih) = 0$$

$$p \mid g_0(i^m m!)^p$$

此与$p > \max(m, |q_0|)$相矛盾．

再证明有一素数$p > \max(m、|g_0|)$，使

$$\left|\sum_{h=0}^{m} g_h Q(ih)\right| < 1$$

则由（2）式引出矛盾，从而e^i不可能是代数数．

据引理和（1）式可得

$$|Q(x)| \leqslant e^{|x|} \sum_{m=0}^{n} |a_m| |x|^m$$

$$\leqslant e^{|x|} \frac{|x|^{p-1} \prod_{h=1}^{m} (h + |x|)^p}{(p-1)!} \tag{3}$$

当固定x且$p\to\infty$时，易证

$$e^{|x|}\frac{|x|^{p-1}\prod_{h=1}^{m}(h+|x|)^{p}}{(p-1)!}\to 0$$

从而（3）式给出　　$|Q(x)|\to 0$

所以任给正有理数$\varepsilon<1$，总可使得

$$|Q(iH)|<\frac{\varepsilon}{(m+1)g}$$

成立。其中

$$|Q(iH)|=\max_{0\leqslant h\leqslant m}|Q(ih)|,\quad g=\max_{0\leqslant h\leqslant m}|g_h|$$

故　$$\left|\sum_{h=0}^{m}g_hQ(ih)\right|\leqslant\sum_{h=0}^{m}|g_h|\,|Q(ih)|\leqslant(m+1)g|Q(iH)|$$

$$<(m+1)g\frac{\varepsilon}{(m+1)g}=\varepsilon<1.$$

上面就证明了e^i是超越数．最后证明sin1是超越数。如果sin1是代数数，则由

$$\cos^2 1=1-\sin^2 1$$

知$\cos^2 1$是代数数，从而可推出cos1是代数数。因此，$e^i=\cos 1+i\sin 1$也是代数数，此与前证e^i是超越数相矛盾。

讨论：以上二题，如果使用提要中定理15进行证明就很简单．

先看习题1．如果

$$\sinh\xi=\frac{e^{\xi}-e^{-\xi}}{2}=\alpha$$

是代数数（ξ为非零有理数），则$2\alpha e^0-e^{\xi}+e^{-\xi}=0$

即　　$e^0, e^{\xi}, e^{-\xi}$

在代数数域上线性相关，此与定理15矛盾．

再看习题2．如果$e^i=\alpha$是代数数，则

$$e^{i} - \alpha e^{0} = 0$$

即

$$e^{i}, \ e^{0}$$

在代数数域上线性相关，也与定理15矛盾.

第十八章　Waring问题及Prouhot-Tarry问题

（略）

第十九章 Шнирельман密率

一、提 要

定义 命**A**表一由一些互不相同的非负整数a所成的集合。命$A(n)$表**A**中不大于n的正整数的个数，即

$$A(n)=\sum_{1\leqslant a\leqslant n}1.$$

若有正数α存在，使对任一正整数n常有

$$A(n)\geqslant \alpha n,$$

则此集合称为有正密率的集合. 有此性质的最大的α称为此集合的正密率。正密率也可称为密率，如果用$d(\mathbf{A})$表示集合**A**的密率，显然有

$$d(\mathbf{A})=\inf_{n\geqslant 1}\frac{\mathbf{A}(n)}{n}.$$

定义 所有形如

$$a+b,\quad a\in\mathbf{A},\quad b\in\mathbf{B}$$

的整数所成的集合称为**A**、**B**的和集，并表示为

$$\mathbf{A}+\mathbf{B}=\mathbf{C}.$$

定理 1 若$\mathbf{C}=\mathbf{A}+\mathbf{B}$及$0\in\mathbf{A}$；$\gamma$，$\alpha$和$\beta$分别表**C**、**A**、**B**的密率，则

$$\gamma\geqslant\alpha+\beta-\alpha\beta.$$

定理 2 若$0\in\mathbf{A}$，$\alpha+\beta\geqslant 1$，则$\mathbf{C}=\mathbf{A}+\mathbf{B}$的密率$\gamma=1$，即是说**C**包含所有正整数。

定理 3　若A包有0，则任一正整数可以表为A中

$$s_0 = 2\left[\frac{\log 2}{-\log(1-\alpha)}\right] + 2$$

个元素的和；若A不包有0，则任一正整数可以表示为A中不多于s_0个元素的和。

定理 4　有一正整数c存在，凡大于1的整数都可表为不超过c个素数的和。

定理 5　设给一M个整数的集合$\{b\}$，能被正整数k所整除的b的个数是

$$\sum_{k \mid b} 1 = g(k)M + R(k).$$

此处$R(k)$是余项，而$g(k)$是正值的积性函数，且$g(p)<1$.

令N_ξ表示$\{b\}$中不能被$\leqslant\xi$的素数所整除的b的个数，则

$$N_\xi \leqslant \frac{M}{\sum\limits_{1\leqslant k\leqslant\xi}\frac{\mu^2(k)}{f(k)}} + \sum_{1\leqslant k_1, k_2\leqslant\xi} \lambda_{k_1}\lambda_{k_2} R\left\{\frac{k_1 k_2}{(k_1, k_2)}\right\}.$$

此处　$$f(k) = \sum_{d \mid k}\mu(d)/g\left(\frac{k}{d}\right)$$

$$\lambda = \frac{\mu(k)}{f(k)g(k)}\sum_{\substack{1\leqslant m\leqslant\xi/k\\(m,k)=1}}\frac{\mu^2(m)}{f(m)}\Big/\sum_{1\leqslant m\leqslant\xi}\frac{\mu^2(m)}{f(m)}.$$

定理定5也可以写成：

定理5′　设给定一个包含N个正整数的集合$\{b\}$，其中能被正整数d整除的个数是

$$\sum_{d \mid b} 1 = \frac{N}{f(d)} + R_d,$$

R为余项，$f(d)$为正值的积性函数。

令N_ξ表$\{b\}$中不能被$\leqslant\xi$的素数所整除的b的个数，则对于正数z有

$$N_\xi \leqslant \frac{N}{\sum\limits_{d\leqslant z}\frac{\mu^2(d)}{g(d)}} + O\Big(\sum_{d_1,d_2\leqslant z}\Big|\lambda_{d_1}\lambda_{d_2}R_{[d_1,d_2]}\Big|\Big).$$

此处
$$g(d) = \sum_{k\mid d}\mu(k)f\left(\frac{d}{k}\right) \neq 0 \qquad (d\leqslant z\leqslant\xi)$$

$$\lambda_d = \mu(d)\frac{f(d)\sum\limits_{\substack{m\leqslant z/d\\(m,d)=1}}\frac{|\mu(m)|}{g(m)}}{g(d)\sum\limits_{m\leqslant z}\frac{|\mu(m)|}{g(m)}} \qquad (d\leqslant z).$$

定理 6 命$A\geqslant 0$，$M\geqslant 3$．设在A与$A+M$之间的素数个数为$\pi(A;M)$，则

$$\pi(A;M)\leqslant\frac{2M}{\log M}\left(1+O\left(\frac{\log\log M}{\log M}\right)\right).$$

此处与O有关的常数与A及M无关。

定理 7 对任一正整数k，有一正整数c存在，凡正整数必为不多于c个正整数的k次乘方的和。

定理 8 若$k\geqslant 2$，$f(x)$为一整系数k次多项式

$$f(x)=a_kx^k+a_{k-1}x^{k-1}+\cdots+a_1x+a_0,$$
$$a_k=O(1),\ a_{k-1}=O(P),\ \cdots,\ a_1=O(P^{k-1}).$$
$$a_0=O(P^k),$$

则

$$\int_0^1\Big|\sum_{x=0}^{P}e^{2\pi if(x)\alpha}\Big|^{8^{k-1}}d\alpha=O(P^{8^{k-1}-k}).$$

二、题 解

§1 密率之定义及其历史

习题 命τ表一实数$\geqslant 1$，求出集合

$$1+[\tau(n-1)], \qquad n=1,2\cdots$$

之密率。

解：下面证明这个集合的密率为$\frac{1}{\tau}$

i）对任一正整数m，都有$\frac{A(m)}{m}\geqslant\frac{1}{\tau}$。

由于对任一整数$a\geqslant 0$，不等式

$$[\tau(a+1)]-[\tau a]\geqslant[\tau a]+[\tau]-[\tau a]$$
$$=[\tau]\geqslant 1$$

恒成立。从而对于任给的正整数m，总可找到整数$b\geqslant 0$，使m满足：

$$[\tau b]<m\leqslant[\tau(b+1)].$$

此时因为 $1+[\tau(1-1)]<m$

$1+[\tau(2-1)]<m$

……

$1+[\tau(b-1)]<m$

$1+[\tau((b+1)-1)]\leqslant m$

且 $1+[\tau((b+2)-1)]>m$

故得 $A(m)=b+1$

所以 $$\frac{A(m)}{m}=\frac{b+1}{m}\geqslant\frac{b+1}{[\tau(b+1)]}\geqslant\frac{1}{\tau}.$$

ii）$\frac{1}{\tau}$是具有性质

$$\frac{A(m)}{m}\geqslant a$$

的最大的a。

对任一正整数m，由

$$1+[\tau(n-1)]\leqslant m$$

有 $n\leqslant\frac{m-1+\delta}{\tau}+1$，$\delta=\{\tau(n-1)\}$，

从而
$$A(m)=\left[\frac{m-1+\delta}{\tau}+1\right]$$

$$\frac{A(m)}{m}=\frac{1}{m}\left[\frac{m-1+\delta}{\tau}+1\right]$$

显然 $\frac{1}{m}\left(\frac{m-1+\delta}{\tau}\right)<\frac{A(m)}{m}\leqslant\frac{1}{m}\left(\frac{m-1+\delta}{\tau}+1\right)$

又因为 $\lim\limits_{m\to\infty}\frac{1}{m}\left(\frac{m-1+\delta}{\tau}\right)=\lim\limits_{m\to\infty}\frac{1}{m}\left(\frac{m-1+\delta}{\tau}+1\right)=\frac{1}{\tau}$

故从夹逼定理立得
$$\lim_{m\to\infty}\frac{A(m)}{m}=\frac{1}{\tau}.$$

上式指出：对于无论多么小的正数ε，当m足够大时总有
$$\frac{A(m)}{m}<\frac{1}{\tau}+\varepsilon.$$

再结合i）证得的$\frac{A(m)}{m}\geqslant\frac{1}{\tau}$，可知$\frac{1}{\tau}$是具有$\frac{A(m)}{m}\geqslant\alpha$性质的最大的$\alpha$。

这样我们就证明了：集合
$$1+[\tau(n-1)],\quad n=1,2,\cdots$$

的密率确为$\frac{1}{\tau}$。

§5 Гольбах-Шнирельман定理之证明

习题 1 设x、k、l都是正整数，且$(k,l)=1$．$\pi(x;k,l)$

表示算术级数$a_n=kn+l$（$n=1, 2, \cdots$）所包含的不超过x的素数的个数，又命δ是满足$0<\delta<1$的固定常数，求证当$k<x^{\delta}$时，有

$$\pi(x;k,l)\leqslant\frac{2x}{\varphi(k)\log\frac{x}{k}}\left(1+O\left(\frac{(\log\log x)^2}{\log x}\right)\right)$$

此处O中所含之常数与k无关，但与δ有关。

证：先证明下面几个引理。

引理1 $\displaystyle\sum_{n\leqslant x}\frac{\Lambda(n)}{n}=\log x+O(1)$.

证：可不妨假定x是整数。

$$\log x!=\sum_{p\leqslant x}\left(\sum_{v\leqslant\left[\frac{\log x}{\log p}\right]}\left[\frac{x}{p^v}\right]\right)\log p$$

$$=\sum_{p\leqslant x}\sum_{v\leqslant\left[\frac{\log x}{\log p}\right]}\frac{x}{p^v}\cdot\log p+O\left(\sum_{p\leqslant x}\left[\frac{\log x}{\log p}\right]\log p\right)$$

$$=x\sum_{n\leqslant x}\frac{\Lambda(n)}{n}+O(\psi(x)).$$

由素数定理 $\psi(x)\sim x$

知道 $O(\psi(x))=O(x)$

再由第五章第八节例2知道

$$\log x!=x\log x+O(x)$$

因此 $$\sum_{n\leqslant x}\frac{\Lambda(n)}{n}=\log x+O(1).$$

引理2

$$\sum_{p\leqslant x}\frac{\log p}{p}=O(\log\log x)\qquad(1)$$

$$\prod_{p|x}\left(1+\frac{1}{p}\right)=O(\log\log x). \tag{2}$$

证：用$\omega(x)$表x的不同素因子的个数，则$2^{\omega(x)}\leqslant x$，故

$$\omega(x)\leqslant\frac{\log x}{\log 2}.$$

由第九章第五节习题1

$$p_n\sim n\log n$$

可得 $$p_n=O(n\log n),$$

再结合 $$\omega(x)\leqslant\frac{\log x}{\log 2}$$

即得 $$p_{\omega(x)}=O(\log x\log\log x)$$

故由上式和引理1就有

$$\sum_{p|x}\frac{\log p}{p}\leqslant\sum_{p\leqslant p_{\omega(x)}}\frac{\log p}{p}\leqslant\sum_{n\leqslant p_{\omega(x)}}\frac{\Lambda(n)}{n}=O(\log\log x)$$

此即（1）式得证。

又设 $$y=\prod_{p|x}\left(1+\frac{1}{p}\right)$$

则 $$\log y=\sum_{p|x}\log\left(1+\frac{1}{p}\right)=\sum_{p|x}\left(\frac{1}{p}-\frac{1}{2p^2}+\frac{1}{3p^3}-\frac{1}{4p^4}+\cdots\right)$$

$$\leqslant\sum_{p|x}\frac{1}{p}\leqslant\sum_{p\leqslant\log x}\frac{1}{p}+\sum_{\substack{p|x\\ p>\log x}}\frac{1}{p} \tag{3}$$

由第五章第九节定理2

$$\sum_{p\leqslant\xi}\frac{1}{p}=\log\log\xi+C+O\left(\frac{1}{\log\xi}\right)$$

得 $$\sum_{p\leqslant\log x}\frac{1}{p}=\log\log\log x+O(1), \tag{4}$$

又因为 $$\sum_{\substack{p\mid x\\ p>\log x}}\frac{1}{p}\leqslant\frac{\omega(x)}{\log x}\leqslant\frac{1}{\log 2} \qquad (5)$$

故把（4）、（5）代入（3）得

$$\log y\leqslant\log\log\log x+O(1)$$

所以 $$y=O(\log\log x)$$

此即（2）式得证。

引理3 若$x\geqslant 3$，则

$$\sum_{d\mid x}\frac{\mu(d)\log d}{d}=O(\log\log x).$$

证：

$$\sum_{d\mid x}\frac{\mu(d)\log d}{d}=\sum_{d\mid x}\frac{\mu(d)}{d}\sum_{p\mid d}\log p$$

$$=\sum_{p\mid x}\log p\sum_{p\mid d}\frac{\mu(d)}{d}=-\sum_{p\mid x}\frac{\log p}{p}\Bigl(\sum_{\substack{t\mid x\\ p\nmid t}}\frac{\mu(t)}{t}\Bigr)$$

$$=-\sum_{p\mid x}\frac{\log p}{p}\Bigl(\sum_{t\mid x}\frac{\mu(t)}{t}-\sum_{\substack{t\mid x\\ p\mid t}}\frac{\mu(t)}{t}\Bigr)$$

$$=-\sum_{p\mid x}\frac{\log p}{p}\Bigl(\frac{\varphi(x)}{x}+\frac{1}{p}\sum_{\substack{t\mid x\\ p\nmid t}}\frac{\mu(t)}{t}\Bigr) \qquad (3)$$

显然，当$p|x$时，

$$\sum_{\substack{t\mid x\\ p\nmid t}}\frac{\mu(t)}{t}=\prod_{\substack{q\mid x\\ q\neq p}}\Bigl(1-\frac{1}{q}\Bigr)=\frac{\varphi(x)}{x}\cdot\frac{1}{1-\frac{1}{p}},\ (q\text{过素数})\qquad (4)$$

故由引理2结合(3)、(4)可得

$$\sum_{d\mid x}\frac{\mu(d)\log d}{d}=-\sum_{p\mid x}\frac{\log p}{p}\Bigl(\frac{\varphi(x)}{x}\cdot\frac{1}{1-\frac{1}{p}}\Bigr)$$

$$= -\frac{\varphi(x)}{x}\sum_{p\mid x}\frac{\lg x}{p-1} = O\left(\sum_{p\mid x}\frac{\log p}{p}\right) = O(\log\log x).$$

此即引理 3 得证。

引理 4　若$x\geqslant 3$是整数而$N\geqslant 1$，则

$$\sum_{\substack{t\leqslant N\\(t,x)=1}}\frac{1}{t} = \frac{\varphi(x)}{x}\cdot\log N + O(\log\log x).$$

证 $$\sum_{\substack{t\leqslant N\\(t,x)=1}}\frac{1}{t} = \sum_{t\leqslant N}\frac{1}{t}\sum_{d\mid(t,x)}\mu(d) = \sum_{d\mid x}\mu(d)\sum_{\substack{d\mid t\\t\leqslant N}}\frac{1}{t} = \sum_{d\mid x}\frac{\mu(d)}{d}\sum_{t\leqslant\frac{N}{d}}\frac{1}{t}$$

$$= \sum_{d\mid x}\frac{\mu(d)}{d}\left(\log\frac{N}{d} + O(1)\right) = \frac{\varphi(x)}{x}\log N$$

$$-\sum_{d\mid x}\frac{\mu(d)\log d}{d} + O\left(\sum_{d\mid x}\frac{|\mu(d)|}{d}\right).$$

故由引理 3 及引理 2 有

$$\sum_{\substack{t\leqslant N\\(t,x)=1}}\frac{1}{t} = \frac{\varphi(x)}{x}\cdot\log N + O(\log\log x) + O\left\{\prod_{p\mid x}\left(1+\frac{1}{p}\right)\right\}$$

$$= \frac{\varphi(x)}{x}\cdot\log N + O(\log\log x).$$

引理 4 由此得证。

作下面的整数集合：

$$M = \left\{a_n \mid a_n = kn + l,\ a_n\leqslant x,\ (k,\ l) = 1\right\}$$

首先，当$(d,\ k) = 1$时

$$\sum_{\substack{kn+l\leqslant x\\d\mid kn+l}} 1 = \left[\frac{x}{k}\right]\frac{1}{d} + R_d,\ |R_d|\leqslant 1$$

当 $(d,\ k) > 1$ 时，上式右边首项为 0，故可在提要定理 5′中令

$\xi = z$ 及 $f(d) = d$

$$g(d) = \sum_{d' \mid d} \frac{\mu(d')}{d'} \cdot d = \varphi(d)$$

于是 $\displaystyle\sum_{1 \leqslant d \leqslant z} \frac{|\mu(d)|}{g(d)} \geqslant \sum_{\substack{1 \leqslant d \leqslant z \\ (d,k)=1}} \frac{|\mu(d)|}{\varphi(d)} = \sum_{\substack{1 \leqslant d \leqslant z \\ (d,k)=1}} \frac{|\mu(d)|}{d \prod_{p \mid d}\left(1 - \frac{1}{p}\right)}$

$$= \sum_{\substack{1 \leqslant d \leqslant z \\ (d,k)=1}} \frac{|\mu(d)|}{d} \prod_{p \mid d} \left(\sum_{a=0}^{\infty} \left(\frac{1}{p}\right)^a \right) \geqslant \sum_{\substack{1 \leqslant d \leqslant z \\ (d,k)=1}} \frac{1}{d}$$

$$= \frac{\varphi(k)}{k} \cdot \log z + O(\log\log(k+3)) .$$

上面最后一步系根据引理4．另一方面

$$R_z \leqslant \left(\sum_{\substack{1 \leqslant d \leqslant z \\ (d,k)=1}} |\lambda_d| \right)^2 \leqslant \left(\sum_{\substack{1 \leqslant d \leqslant z \\ (d,k)=1}} \frac{|\mu(d)| \cdot |f(d)|}{|g(d)|} \right)^2$$

$$\leqslant \left(\sum_{1 \leqslant d \leqslant z} \frac{|\mu(d)|}{\prod_{p \mid d}\left(1 - \frac{1}{p}\right)} \right)^2 \leqslant \left(\sum_{1 \leqslant d \leqslant z} 2^{\omega(d)} \right)^2$$

$$\leqslant \left(\sum_{1 \leqslant d \leqslant z} \tau(d) \right)^2 = O(z^2 \log^2 z)$$

取 $\quad z = \dfrac{\left(\frac{x}{k}\right)^{\frac{1}{2}}}{\log^2 x}$ ，

则由定理5′及引理2和已知 $k < x^{\delta}$， $0 < \delta < 1$ 有

$$N_z \leqslant \frac{\frac{x}{k}}{\frac{\varphi(k)}{k} \log z \left(1 + O\left(\frac{k}{\varphi(k)} \cdot \frac{\log\log(k+3)}{\log z} \right) \right)}$$

$$+ O(z^2 \log^2 z)$$

$$\leqslant \frac{2x}{\varphi(k)\log\frac{x}{k}}\left(1+O\left(\frac{(\log\log x)^2}{\log x}\right)\right)$$

再由 $\pi(x;\ k,\ l)=\sum_{\substack{kn+l\leqslant x\\ p=kn+l>z}}1+\sum_{\substack{kn+l\leqslant x\\ p=kn+l\leqslant z}}1\leqslant N_z+z$

可得 $\pi(x;\ k,\ l)\leqslant\frac{2x}{\varphi(k)\log\frac{x}{k}}\left(1+O\left(\frac{(\log\log x)^2}{\log x}\right)\right)$.

习题 2 若p、$p+2$同时为素数，则p与$p+2$就称做一对"孪生素数"。以$Z_2(N)$表示小于或等于N的"孪生素数"的对数，则

$$Z_2(N)\leqslant c_8\frac{N}{\log^2 N}.$$

并证明级数

$$\sum_{p^*}\frac{1}{p^*}$$

收敛，此处p^*经过所有的"孪生素数"，即p^*与p^*-2是一对"孪生素数"。

证：考虑三个数列

$$q_1,\ q_2,\ q_3,\ \cdots,\quad (q_1<q_2<\cdots)$$

$$a_1,\ a_2,\ a_3,\ \cdots,\quad (0\leqslant a_i<q_i)$$

$$b_1,\ b_2,\ b_3,\ \cdots,\quad (0\leqslant b_i<q_i)$$

其中 $q_1,\ q_2,\ q_3,\ \cdots$

是全体素数所组成的序列中删去了2、d的素因数，及有限个(个数可以是0)其它任意指定的素数后所剩下的素数。我们利用每一个q_i作公差，可以造出两组等差级数。

$$a_i+mq_i,\ b_i+mq_i,\ m=0,\ 1,\ 2,\ \cdots$$

我们考虑满足$q_i \leqslant y$的q_i，并用$\pi'(y)$表示这些q_i的个数。我们要从等差级数F内（F表示以$a>0$为首项，$d>0$，$a<d$，d为公差的一个等差级数）不超以x的一段里筛去一切包含在上述$2\pi'(y)$个等差级数中的项。显然，所筛剩下来的n满足：

$$n \leqslant x \text{及} n \not\equiv a_i (\bmod q_i),\quad n \not\equiv b_i (\bmod q_i)\ (i \leqslant \pi'(y)).$$

今用$N(d, x, y)$表示如此筛剩下来的个数。下面我们将证明：当$u \geqslant 2$及x充分大时有

$$N(d, x, x^{\frac{1}{u}}) \leqslant \frac{A_2 x}{\log^2 x}.$$

今先假定$a_i \not\equiv b_i (\bmod q_i)$，$i = 1, 2, \cdots, k$。

容易看出 $N(d, x, q_{k-1}) - N(d, x, q_k)$

就是满足下列条件的m的个数：

$$m \leqslant x,\ m \equiv a (\bmod d),\ m \equiv a_k \text{或} \equiv b_k (\bmod q_k),$$

$$(m - a_i)(m - b_i) \not\equiv 0 (\bmod q_i),\ i = 1, 2, \cdots, k-1.$$

由于$(d, q_i) = 1$，由孙子定理，可以找到a'及a''（$0 \leqslant a' < dq_k$，$0 \leqslant a'' < dq_k$）使得以上的条件可以改写成下面的形式：

$$m \leqslant x,\ m \equiv a' \text{或} a'' (\bmod q_k)$$

$$(m - a_i)(m - b_i) \not\equiv 0 (\bmod q_i), i = 1, 2, \cdots, k-1. \qquad (1)$$

若用$N(dq_k, x, q_{k-1}, a')$

及

$$N(dq_k, x, q_{k-1}, a'')$$

分别表 $m \equiv a'$及$m \equiv a'' (\bmod dq_k)$

时（1）的解数，那么（1）的总解数就是：

$$N(dq_k, x, q_{k-1}, a') + N(dq_k, x, q_{k-1}, a'') \qquad (2)$$

但由于我们所要推出的结果，实际上并不受a'及a''不同的影响，因而我们可以更笼统的用下面符号表示（1）的总解数：

$$2N(dq_k, x, q_{k-1})$$

于是我们有：

$$N(d,\ x,\ q_k)=N(d,\ x,\ q_{k-1})-2N(dq_k,\ x,\ q_{k-1}) \qquad (3)$$

当$k=1$时，上式右边应写作

$$N(d,\ x)-2N(dq_1,\ x),$$

其中$N(d,\ x)$表示某一公差是d的等差级数中不超过x的项数，不论首项怎样，都有

$$N(d,\ x)=\frac{x}{d}+\theta,\ |\theta|\leqslant 1 \qquad (4)$$

为简便计，下面用$N(y,\ x,\ q_0)$代表$N(y,\ x)$。首先从（3）得

$$N(d,\ x,\ q_k)=N(d,\ x,\ q_{k-2})-2N(dq_{k-1},\ x,\ q_{k-2})$$

$$-2N(dq_k,\ x,\ q_{k-1})$$

$$=\cdots=N(d,\ x)-2\sum_{r_1\leqslant k}N(dq_{r_1},\ x,\ q_{r_1-1}) \qquad (5)$$

其次，同样处理（5）右端$\sum$号每一项，结果得到

$$N(d,\ x,\ q_k)=N(d,\ x)-2\sum_{r_1\leqslant k}N(dq_{r_1},\ x)$$

$$+4\sum_{r_1\leqslant k}\sum_{r_2<r_1}N(dq_{r_1}q_{r_2},x,q_{r_2-1}) \qquad (6)$$

一般地，当$t\leqslant k$时有：

$$N(d,x,q_k)=N(d,x)-2\sum_{r_1\leqslant k}N(dq_{r_1},\ x)+$$

$$+4\sum_{r_1\leqslant k}\sum_{r_2<r_1}N(dq_{r_1}q_{r_2},\ x)-$$

$$-8\sum_{r_1\leqslant k}\sum_{r_2<r_1}\sum_{r_3<r_2}N(dq_{r_1}q_{r_2}q_{r_3},x)+\cdots$$

$$+(-2)^t\sum_{r_1\leqslant k}\cdots\sum_{r_t<r_{t-1}}N(dq_{r_1}\cdots q_{r_t},x,q_{r_t-1})\text{.} \qquad (7)$$

在（7）中取$t=3$得：

$$N(d, x, q_k) = N(d, x) - 2\sum_{r_1 \leqslant k} N(dq_{r_1}, x) +$$

$$+ 4\sum_{r_1 \leqslant k}\sum_{r_2 < r_1} N(dq_{r_1}q_{r_2}, x)$$

$$- 8\sum_{r_1 \leqslant k}\sum_{r_2 < r_1}\sum_{r_3 < r_2} N(dq_{r_1}q_{r_2}q_{r_3}, x, q_{r_3 - 1}) \qquad (8)$$

为了减少（8）中各项所包含的总项数，我们用不等式$r_3 \leqslant k_1$去限制r_3的变化，因删去的每一项$\leqslant 0$，结果得到

$$N(d, x, q_k) \leqslant N(d, x) - 2\sum_{r_1 \leqslant k} N(dq_{r_1}, x)$$

$$+ 4\sum_{r_1 \leqslant k}\sum_{r_2 < r_1} N(dq_{r_1}q_{r_2}, x)$$

$$- 8\sum_{r_1 \leqslant k}\sum_{r_2 < r_1}\sum_{r_3 < r_2} N(dq_{r_1}q_{r_2}q_{r_3}, x, q_{r_3 - 1}) \qquad (9)$$

利用（6）式，把上面最后一项改变一下得到：

$$N(d, x, q_k) \leqslant N(d, x) - 2\sum_{r_1 \leqslant k} N(dq_{r_1}, x)$$

$$+ 4\sum_{r_1 \leqslant k}\sum_{r_2 < r_1} N(dq_{r_1}q_{r_2}, x)$$

$$- 8\sum_{r_1 \leqslant k}\sum_{r_2 < r_1}\sum_{\substack{r_3 < r_2 \\ r_3 \leqslant k_1}} N(dq_{r_1}q_{r_2}q_{r_3}, x)$$

$$+ 16\sum_{r_1 \leqslant k}\sum_{r_2 < r_1}\sum_{\substack{r_3 < r_2 \\ r_3 \leqslant k_1}}\sum_{r_4 < r_3} N(dq_{r_1}q_{r_2}q_{r_3}q_{r_4}, x)$$

$$- 32\sum_{r_1 \leqslant k}\sum_{r_2 < r_1}\sum_{\substack{r_3 < r_2 \\ r_3 \leqslant k_1}}\sum_{r_4 < r_3}\sum_{\substack{r_5 < r_4 \\ r_5 \leqslant k_2}} N(dq_{r_1}q_{r_2}q_{r_3}q_{r_4}q_{r_5}, x, q_{r_5 - 1}) \qquad (10)$$

注意到我们在$r_5 < r_4$下面加上了$r_5 \leqslant k_2$，这个限制只有使上式右边增大，因此不等式成立。同样，我们又可以利用（6）去改变

(10) 的最后一项，同时又添加限制$r_7 \leqslant k_3$。这种办法显然可以继续进行，只要$2s+1 \leqslant k$，就可以得到

$$N(d,x,q_n) \leqslant N(d,x) - 2\sum_{r_1 \leqslant k} N(dq_{r_1},x) + \cdots$$

$$+ 2^{2v}\sum_{r_1 \leqslant k}\sum_{r_2<r_1}\cdots\sum_{\substack{r_{2v-1}<r_{2v-2}\\ r_{2v-1}\leqslant k_{v-1}}}\sum_{r_{2v}<r_{2v-1}} N(dq_{r_1}\cdots q_{r_{2v}},x)$$

$$- 2^{2v+1}\sum_{r_1 \leqslant k}\sum_{r_2<r_1}\cdots\sum_{r_{2v}<r_{2v-1}}\sum_{\substack{r_{2v+1}<r_{2v}\\ r_{2v+1}\leqslant k_v}} N(dq_{r_1}\cdots q_{r_{2v+1}},x) + \cdots$$

$$+ \cdots - 2^{2s+1}\sum_{r_1 \leqslant k}\sum_{r_2<r_1}\cdots\sum_{r_{2s}<r_{2s-1}}\sum_{\substack{r_{2s+1}<r_{2s}\\ r_{2s+1}\leqslant k_s}} N(dq_{r_1}\cdots q_{r_{2s+1}},x,q_{r_{2s+1}-1}) \qquad (11)$$

最后假定$2s+2 \leqslant k$，我们就可以利用（5）变上面最后一项为(注意到$2s+2 \leqslant k$)：

$$- 2^{2s+1}\sum_{r_1 \leqslant k}\sum_{r_2<r_1}\cdots\sum_{r_{2s}<r_{2s-1}}\sum_{\substack{r_{2s+1}<r_{2s}\\ r_{2s+1}\leqslant k_s}} N(dq_{r_1}\cdots q_{r_{2s+1}},x)$$

$$+ 2^{2s+2}\sum_{r_1 \leqslant k}\sum_{r_2<r_1}\cdots\sum_{\substack{r_{2s+1}<r_{2s}\\ r_{2s+1}\leqslant k_s}}\sum_{r_{2s+2}<r_{2s+1}} N(dq_{r_1}\cdots q_{r_{2s+2}},x,q_{r_{2s+2}-1}).$$

上面第二项是正的，因此利用（5）可以把

$$N(dq_{r_1}\cdots q_{r_{2s+2}}, x, q_{r_{2s+2}-1})$$

换成 $N(dq_{r_1}\cdots q_{r_{2s+2}}, x)$

故可得 $$N(d,x,q_k)<\frac{x}{d}E+R \tag{12}$$

其中

$$E=1-\sum_{r_1\leqslant k}\left(2q_{r_1}^{-1}\right)+\sum_{r_1\leqslant k}\sum_{r_2<r_1}\left(2q_{r_1}^{-1}\right)\left(2q_{r_2}^{-1}\right)$$
$$-\cdots+(-1)^{2s+2}\sum_{r_1\leqslant k}\sum_{r_2<r_1}\cdots\sum_{\substack{r_{2s+1}<r_{2s}\\ r_{2s+1}\leqslant k_s}}\sum_{r_{2s+2}<r_{2s+1}}$$
$$\left(2q_{r_1}^{-1}\right)\cdots\left(2q_{r_{2s+1}}^{-1}\right) \tag{13}$$

已有

$$r_{2j+2}\leqslant k_j, r_{2j+1}\leqslant k_j \quad (j=0,1,2,\cdots,s),$$
$$1\leqslant r_{2s+2}<r_{2s+1}<\cdots<r_2<r_1\leqslant k \tag{14}$$

还假定 $$1\leqslant k\leqslant k_{-1}\leqslant\cdots\leqslant k_1\leqslant k_0=k \tag{15}$$

显然E的各项都包含在下列乘积的展开式中：

$$\left(1-2\sum_{r_1\leqslant k}q_{r_1}^{-1}\right)\left(1-2\sum_{r_2\leqslant k}q_{r_2}^{-1}\right)\cdots$$
$$\cdots\cdots\left(1-2\sum_{r_{2s+1}\leqslant k_s}q_{r_{2s+1}}^{-1}\right)\left(1-2\sum_{r_{2s+2}\leqslant k_s}q_{r_{2s+2}}^{-1}\right)$$

因此不难看出

$$|R|\leqslant(2k_0+1)^2(2k_1+1)^2\cdots(2k_s+1)^2 \tag{16}$$

用$E^{(i)}$表示（13）式右边i重和数，即

$$E^{(i)}=\sum_{r_1}\sum_{r_2}\cdots\sum_{r_i}\left(2q_{r_1}^{-1}\right)\cdots\left(2q_{r_i}^{-1}\right) \tag{17}$$

其中r_1，…，r满足（14）式。令$E^{(0)}=1$，又用E_m表（13）右

边满足

$$r_\mu > k_m \quad (\mu = 1,\ 2,\ \cdots,\ \nu) \tag{18}$$

的各项 $(2q_{r_1}^{-1})\cdots(2q_{r_\nu}^{-1})$ 的和．由（14）式知道$\mu \leqslant 2m$时(18)才有可能成立，因此当$i > 2m$时，$E^{(i)}$不包含满足条件(18)的项．

今用$E_m^{(i)}$表示出现在E_m内及$E^{(i)}$中的各公共项的和，则有

$$E_m^{(i)} = 0 \qquad (\text{当} i > 2m \text{时})$$

及

$$E_m = \sum_{i=0}^{2m} (-1)^i E_m^{(i)} \qquad (\text{此处} E_m^{(0)} = 1) \tag{19}$$

为便利计，令$k_{s+1} = 0$，则

$$E = E_{s+1} \tag{20}$$

根据E_m的定义，q_1，q_2，…，q_{k_m}

诸素数是不在E_m中出现的，因此从E_m过渡到E_{m+1}时，必须添进$N = k_m - k_{m+1}$个素数：

$$q_z,\ (k_{m+1} < z \leqslant k_m)$$

今用$S_{m+1}^{(\mu)}$表示这N个数$2q_z^{-1}$的第μ个初等函数，即

$$S_{m+1}^{(\mu)} = \sum_{k_m > z_1 > z_2 > \cdots\cdots > z_\mu > k_{m+1}} \cdots\cdots\cdots \sum \left(2q_{z_1}^{-1}\right)\cdots\left(2q_{z_\mu}^{-1}\right)$$

则有

$$E_{m+1}^{(i)} = \sum_{r_1} \cdots \sum_{i}^{(m+1)} \left(2q_{r_1}^{-1}\right)\left(\cdots 2q_{i}^{-1}\right)$$

其中$\sum$上面的$m+1$表示r_1，…，r_i满足不等式（看（14）式及（18）式）

$$\begin{gathered} 1 \leqslant r_j < r_{j-1} < r_1 \qquad (j = 3,\ 4,\ \cdots) \\ k_{m+1} < r_j \leqslant k_{\left[\frac{1}{2}(j-1)\right]} \end{gathered} \tag{21}$$

当$j\leqslant 2m+2$时，由 $k_{m+1}<r_j\leqslant k_m$可推出（21），故当$i\leqslant 2m+2$时，有

$$E_{m+1}^{(i)}=\sum_{\nu=0}^{i} S_{m+1}^{(i-\nu)} E_m^{(\nu)}$$

$$E_{m+1}=\sum_{i=0}^{2m+2}\sum_{\nu=0}^{i}(-1)^i S_{m+1}^{(i-\nu)} E_m^{(\nu)} \tag{22}$$

其中当$\mu>N$时，

$$S_{m+1}^{(\mu)}=0.$$

另一方面，我们有（注意$\beta>N$时或$\alpha>2m$时，$E_m^{(\alpha)}E_{m+1}^{(\beta)}=0$）

$$\begin{aligned}
E_m &= \prod_{k_{m+1}<z\leqslant k_m}\left(1-2q_z^{-1}\right)\\
&=\sum_{\alpha=0}^{2m}\sum_{\beta=0}^{N}(-1)^{\alpha+\beta}E_m^{(\alpha)}S_{m+1}^{(\beta)}\\
&=\sum_{i=0}^{N+2m}\sum_{\nu=0}^{i}(-1)^i E_m^{(\nu)} S_{m+1}^{(i-\nu)}.
\end{aligned}$$

比较（22）式，令$\tau=i-2m$，并注意到$\nu>2m$时，$E_m^{(\nu)}=0$，即得

$$E_{m+1}=E_m\prod_{k_{m+1}<z\leqslant k_m}\left(1-2q_z^{-1}\right)-\sum_{\tau=3}^{N}(-1)^\tau\sum_{\nu=0}^{2m}E_m^{(\nu)}S_{m+1}^{(2m+\tau-\nu)} \tag{23}$$

上面已经假定了$N\geqslant 3$，这是由于当$N=2$时显然有

$$E_{m+1}=E_m\prod_{k_{m+1}<z\leqslant k_m}\left(1-2q_z^{-1}\right) \tag{24}$$

又当$N=1$时，不难看出（22）式内第二等式右边相当于$i=2m+2$的项都等于0，因此（24）式仍然成立。

我们要证明，可以适当地选择筛数k_j，使得（23）式内二重和中相当于$\tau=3$，4，…，N的各单重和的绝对值是递减的。这样，二重和的绝对值就小于第一个单重和（即相当于$\tau=3$的那一项），因而

$$E_{m+1}<E_m\prod_{k_{m+1}<z\leqslant k_m}\left(1-2q_z^{-1}\right)+\sum_{\nu=0}^{2m}E_m^{(\nu)}S_{m+1}^{(2m+3-\nu)}. \tag{25}$$

由(23)式可以看出，上式当$N(=k_m-k_{m+1})=1$或2时，便可省去右边第二项。剩下的问题只有选择筛数k_j使得(23)式内二重和中相当于$\tau=3$，4，…，N的各单重和的确是递减的。

由于$S_{m+1}^{(g)}$内每一项都可以表成$S_{m+1}^{(1)}$中的一项与$S_{m+1}^{(g-1)}$中的一项的积，表示的方法个数是g，因此

$$S_{m+1}^{(g)}\leqslant\frac{S_{m+1}^{(1)}}{g}\cdot S_{m+1}^{(g-1)} \tag{26}$$

今后要选定筛数k_j，使得：

$$S_{m+1}^{(1)}=\sum_{k_{m+1}<z\leqslant k_m}2q_z^{-1}<1 \tag{27}$$

如此就可以得到

$$S_{m+1}^{(g)}<S_{m+1}^{(g-1)}$$

从而立刻可以看出(23)式内二重和中各单重和的递减性。从(26)、(27)还可以看出：

$$S_{m+1}^{(g)}\leqslant\frac{\left(S_{m+1}^{(1)}\right)^g}{g!} \tag{28}$$

我们先取定 ρ、ρ_0 两个数，使得：

$$\rho_0 > \rho > 1, \quad 0 < 2\log\rho_0 < 1 \tag{29}$$

设当$m \leqslant M$时，我们令

$$k_m = \pi'\left(q_k^{1/\rho^m}\right) \tag{30}$$

则 当$k_{m+1} < z \leqslant k_m$ 时，

$$q_k^{1/\rho^{m+1}} < q_z \leqslant q_k^{1/\rho^m} \tag{31}$$

由(10)式和习题 1 证明中引理 2 所引的公式以及Bertrand假设(n与$2n$之间至少有一个素数)，我们不难看 出，当$k_m \to \infty$时，

$$\frac{1}{2} S_{m+1}^{(1)} = \sum_{k_{m+1} < z \leqslant k_m} q_z^{-1} = \log\rho + o(1)$$

$$P_{m+1} = \prod_{k_{m+1} < z \leqslant k_m} (1 - 2q_z^{-1}) = \frac{1 + o(1)}{\rho^2} \tag{32}$$

注意：我们在这里用到了前面所说q_1，q_2，…，是从一切素数中删去有限个而得到的。

因此，我们可以找到只与ρ及ρ_0有关的ω，同时就找到一个正整数M，使得当 $q_{k_m} > q_{k_{m+1}} > \omega$时，或者说当$m \leqslant M$ 时，(32)内的两个$o(1)$都相当小，以致

$$S_{m+1}^{(1)} < 2\log\rho_0 < 1, \quad P_{m+1} > \rho_0^{-2} \tag{33}$$

这说明当$m \leqslant M$时，满足了（27）式的要求。我们还需 考虑一下不 超过ω的有限个素数 q_i（这也就是满 足$i \leqslant k_{M+1}$的 q_i ）。我们把指标i依下列方法分段：

$$k_{c+1} < i \leqslant k_c, \quad c \geqslant M+1,$$

$$k_c - k_{c+1} = 1 \text{或} 2.$$

在这种情况下，（27）式已经不起作用，因为(25)式右边第二项已经可以略去了(参看(25)式下面一段话)。

首先让我们来估计 $E = E_{s+1}$(参看(20)式)。(25) 右面第二

项是

$$\sum=\sum_{v=0}^{2m} E_m^{(v)} S_{m+1}^{(2m-3-v)}.$$

其中 $E_m^{(v)} = \sum_{r_1}\cdots\sum_{r_v}(2q_{r_1}^{-1})\cdots(2q_{r_v}^{-1}) \qquad (v\leqslant 2m)$

(m)表示有下列不等式

$$1\leqslant r_j<r_{j-1}<r_1 (j=3, 4\cdots)$$

$$km<r_j\leqslant k[\tfrac{1}{2}(j-1)] (\text{有 } 0\leqslant[\tfrac{1}{2}(j-1)]\leqslant m-1).$$

而 $S_{m+1}^{(\mu)}=\sum_{k_m\geqslant z_1>z_2>\cdots>z_\mu>k_{m+1}}\cdots\cdots\cdots\cdots\cdots\cdots\sum\left(2q_{z_1}^{-1}\right)\cdots\left(2q_{z_\mu}^{-1}\right)$

注 意到当$v>2m$时$E_m^{(v)}=0$及当$v>0$时$E_0^{(v)}=0$，于是有

$$\sum=\sum_{v=0}^{2m} E_m^{(v)} S_{m+1}^{(2m+3-v)}=\sum_{v=0}^{2m} S_{m+1}^{(2m+3-v)}\sum_{j=0}^{v} S_m^{(v-j)} E_{m-1}^{(j)}$$

$$=\sum_{v=0}^{2m} S_{m+1}^{(2m+3+v)}\sum_{j=0}^{v} S_m^{(v-j)}\sum_{l=0}^{j} S_{m+1}^{(j-l)} E_{m-2}^{(l)}=\cdots$$

$$=\sum_{v_1=0}^{2m} S_{m+1}^{(2m+3-v_1)}\sum_{v_2=0}^{v_1} S_m^{(v_1-v_2)}\cdots\sum_{v_{m+1}=0}^{v_m} S_1^{(v_m-v_{m+1})} E_0^{(v_{m+1})}$$

$$=\sum\sum_{v_1+v_2+\cdots+v_{m+1}=2m+3}\cdots\cdots\sum S_{m+1}^{(v_1)} S_m^{(v_2)}\cdots S_1^{(v_{m+1})}.$$

又

$$S_{m+1}^{(g)}\leqslant\frac{\left(S_{m+1}^{(1)}\right)^g}{g!}$$

故 $\sum\leqslant\sum_{v_1+v_2+\cdots+v_{m+1}=2m+3}\frac{\left(S_{m+1}^{(1)}\right)^{v_1}\left(S_m^{(1)}\right)^{v_2}\cdots\left(S_1^{(1)}\right)^{v_{m+1}}}{v_1!\cdots\cdots\cdots\cdots v_{m+1}!}$

$$=\frac{1}{(2m+3)!}\left(S_1^{(1)}+\cdots+S_{m+1}^{(1)}\right)^{2m+3}$$

利用不等式 $\frac{1}{\nu!}<\frac{1}{\nu^\nu}e^\nu$

即得 $$\sum<\frac{1}{(2m+3)^{2m+3}}e^{2m+3}\left((m+1)2\log\rho_0\right)^{2m+3}$$

$$=\left(\frac{2(m+1)e\log\rho_0}{2m+3}\right)^{2m+3}$$

$$<(e\log\rho_0)^{2m+3}=\tau^{2m+3}$$

此处 $\tau=e\log\rho_0$

因此当(33)式成立时，由(25)得：

$$E_{m+1}<E_m\prod_{k_{m+1}<z\leqslant k_m}(1-2q_z^{-1})+\tau^{2m+3}$$

$$<P_{m+1}(E_m+\tau^{2m+3}\rho_0^{\ 2}).$$

接连应用上述不等式，并注意到$E_0=1$，可得

$$E_{m+1}<P_{m+1}P_m\cdots P_1\{1+\tau^3\rho_0^{\ 2}+\cdots+\tau^{2m+3}\rho_0^{\ 2m+2}\}$$

选择ρ_0时，若同时满足

$$\tau\rho_0=e\rho_0\log\rho_0<1$$

则 $$E_{m+1}<\delta P_{m+1}P_m\cdots P_1$$

$$\delta=\frac{\tau^3\rho_0^{\ 2}}{1-\tau^2\rho_0^{\ 2}}+1 \tag{34}$$

当$c\geqslant M+1$时，由于前面对k_c及k_{c+1}的选择，我们可以得到

$$E_{c+1}<E_c P_{c+1}$$

这时（33）式虽然不见得成立，但也没有多大关系了。总之，我们得到了

$$E=E_{s+1}<\delta\prod_{\nu=1}^{k}(1-2q_\nu^{-1}) \tag{35}$$

$$\delta=\frac{\tau^{3}\rho_0{}^{2}}{1-\tau^{2}\rho_0{}^{2}}+1$$

其次，我们要估计R。因$q\geqslant 3$，故$2m+1\leqslant q_m$常成立，由(16)式即得

$$|R|\leqslant q^2{}_{k_0}q^2{}_{k_1}\cdots q^2{}_{k_M}q^2{}_{k_{M+1}}\cdots q^2{}_{k_s}\leqslant q_k^Q q^2{}_{k_{M+1}}\cdots q^2{}_{k_s}$$
$$=q_k{}^Q A$$

其中A只与ρ、ρ_0有关，因而$q_{k_m}\leqslant q_k^{1/\rho m}$（参看(31)式），且有

$$Q=2+2\rho^{-1}+\cdots+2\rho^{-M}=\frac{2(\rho-\rho^{-M})}{\rho-1}<\frac{2\rho}{\rho-1}$$

因此

$$|R|<Aq_k{}^{2\rho/(\rho-1)} \qquad (36)$$

今取$k=\pi'\left(x^{\frac{1}{u}}\right)$，则由(36)式得：

$$|R|\leqslant Ax^{f}\quad ,\quad f=\frac{2\rho}{(\rho-1)u}$$

又由（35）式及

$$\prod_{r=1}^{k}\left(1-2q_r^{-1}\right)\sim\frac{ku^2}{\log^2 x}\quad (k\text{是一常数})$$

(上式成立是因为

$$k=\pi'\left(x^{\frac{1}{u}}\right)\sim\pi\left(x^{\frac{1}{u}}\right)\sim ux^{\frac{1}{u}}\Big/\log x,$$

$$\prod_{2<p\leqslant x}\left(1-\frac{2}{p}\right)=\frac{A+o(1)}{\log^2 x}.\ )$$

可得：
$$E\leqslant\frac{\delta A_1u^2}{\log^2 x}\quad (A_1\text{为一常数})$$

因此由(8)～(16)得：

$$N(d,x,x^{\frac{1}{u}}) < \frac{A_1\delta u^2}{d}\cdot\frac{x}{\log^2 x} + Ax^f$$

$$= A_1\frac{\delta u^2}{d}\cdot\frac{x}{\log^2 x}\left\{1+\frac{Ad}{A_1\delta u^2}\cdot\frac{\log^2 x}{x^{1-f}}\right\} \tag{37}$$

若$f<1$，则上面花括号中的式子是$1+o(1)$，例如我们取

$$\rho=\frac{5}{4}=1.25,\quad u=11$$

即得$f<1$，如果再取$\rho_0=1.2501$，则$\tau\rho_0=e\rho_0\log\rho_0\approx0.758$，而以前(17)～(36)中所有要求都已满足。又由计算可得$\delta\approx1.82$。显然(37)式右边花括号内的数值当$u\geqslant11$时是随x的增大而趋于1的。反过来看，假定x先固定而u的值减少，那么由于筛子用的素数q_i增多了，$N(d,\ x,\ x^{\frac{1}{u}})$决不会随$u$的减少而增多。因此，我们可以断言：当$u\geqslant2$及$x$充分大时有

$$N(d,x,x^{\frac{1}{u}})\leqslant\frac{A_2x}{\log^2 x} \tag{38}$$

下面再估计不超过N的奇数（即取$a=1$，$d=2$）中所含“孪生素数”的个数，也就是说要估计满足下列各条件的个数$Z_2(N)$：

$n\leqslant N$，$n\equiv1\pmod 2$，$n\not\equiv0\pmod{p_i}$，

$n-2\not\equiv0\pmod{p_i}$，$2<p_i\leqslant\sqrt{N}$。

取$a_i=0$，$b_i=2$，$q_i=p_{i+1}$，当N充分大时，由(38)得：

$$Z_2(N)=N(d,\ N,N^{\frac{1}{2}})+Z_2(\sqrt{N}+2)\leqslant\frac{A_2N}{\log^2 N}$$

$$+\sqrt{N}+2\leqslant\frac{c_8N}{\log^2 N}.$$

式中A_2、c_8都是正常数。

最后证明$\sum_{p'}\frac{1}{p'}$是收敛的。若令p_m表第m对“孪生素数”中的

较大者，则

$$m<\frac{c_8 p_n}{\log^2 p_m}$$

或者 $$\frac{1}{p_n}<\frac{c_8}{m\log^2 p_m}<\frac{c_8}{m\log^2 m}.$$

因为级数

$$\sum_{m=2}^{\infty}\frac{1}{m\log^2 m}$$

是收敛的，故由比较判定法可知级数$\sum_p \frac{1}{p}$也是收敛的。

§6 Waring-Hilbert定理

习题 从定理 4 推出定理 5 .

证：此题要求证明：当$k\geqslant 2$时，如果

$$\sum_{1\leqslant a\leqslant n} r^2(a)\ll n^{\frac{2c_1}{k}-1}$$

则一定有

$$\int_0^1\left|\sum_{x=0}^{P} e^{2\pi i x^k \alpha}\right|^{2c_1}\ll P^{2c_1-k}.$$

这里 $r(a)$为

$$x_1^k+x_2^k+\cdots+x_{c_1}^k=a,\ \ x_m\geqslant 0$$

的解数；$c_1=\frac{1}{2}\cdot 8^{k-1}$，而$\ll$中所含的常数只与$k$有关。

$$\int_0^1 \left|\sum_{x=0}^{P} e^{2\pi i x^k \alpha}\right|^{2c_1} d\alpha$$

$$= \int_0^1 \left|\sum_{x_1=0}^{P} \cdots \sum_{x_{c_1}=0}^{P} e^{2\pi i (x_1^k + \cdots + x_{c_1}^k)\alpha}\right|^2 d\alpha$$

$$= \int_0^1 \left| \sum_{0 \leqslant a \leqslant c_1 P^k} e^{2\pi i a\alpha} \sum_{\substack{k_1^k + \cdots + x_{c_1}^k = a \\ 0 \leqslant x_i \leqslant P \\ 1 \leqslant i \leqslant c_1}} 1 \right|^2 d\alpha$$

$$= \sum_{0 \leqslant a \leqslant c_1 P^k} \Big(\sum_{\substack{x_1^k + \cdots + x_{c_1}^k = a \\ 0 \leqslant x \leqslant P \\ 1 \leqslant i \leqslant c_1}} 1 \Big)^2 \ll \sum_{0 \leqslant a \leqslant c_1 P^k} r^2(a)$$

$$\ll \left(P^k\right)^{\frac{2c_1}{k} - 1} = P^{2c_1 - k}.$$

第二十章　数的几何

一、提　　要

定义　命c表平面上一简单封闭曲线，称此曲线在平面上所围的部分R为域；若域R中任意两点的连线恒在R中，则称此域为凸域。

定理 1　平面上一个以原点为对称中心的凸域R，其面积若大于4，则其中必包有一异于原点的整点；若面积大于或等于4，则此一整点在R内或在边界上。

定义　R为n维空间中的有限域，如连接R内任意两点的线段全在R内，则称R为n维凸域。

定理 2　在n维空间中任一以原点为对称中心且体积$>2^n$的凸域R，必包有一异于原点的整点；若体积$\geqslant 2^n$，则此一整点在R内或在边界上。

定理 3　若ξ_1，…，ξ_n是具有实系数的几个变数x_1,…，x_n的线性式，其系数行列式是Δ；λ_1，…，λ_n是n个正数且

$$\lambda_1\cdots\lambda_n\geqslant|\Delta|,$$

则有非全为零的整数x_1，…，x_n，使得

$$|\xi_1|\leqslant\lambda_1,\ |\xi_2|\leqslant\lambda_2,\ \cdots,\ |\xi_n|\leqslant\lambda_n.$$

定理 4　必有一组整数$x_1\cdots$，x 及y，不全为零，使

$$|a_1x_1+\cdots+a_nx_n+y|<\frac{1}{t}$$

而 $|x_v|\leqslant t^{\frac{1}{n}}$ （此处 t 为任一正实数）．

定理5 命a_1，$\cdots a_n$为一组实数及 $t\geqslant 1$，则必有一异于原点的整点

$$(x, y_1, \cdots, y_n)$$

使得 $$|a_v x - y_v|<\frac{1}{t}, \quad 1\leqslant x\leqslant t^n.$$

定理6 n 维空间内半径为 r 的球体体积为

$$r^n\frac{\pi^{\frac{1}{2}n}}{\Gamma(\frac{1}{2}n+1)}.$$

定理7 若 $Q(x_1, \cdots, x_n)$是一定正型，其行列式为D，则有一异于原点的整点$(x_1, \cdots, x_n)$使

$$Q(x_1, \cdots, x_n)\leqslant 4J_n^{-\frac{2}{n}}D^{\frac{1}{n}}$$

其中 $$J_n=\frac{\pi^{\frac{1}{2}n}}{\Gamma(\frac{1}{2}n+1)}.$$

定理8 设 $\xi_1, \cdots, \xi_n$是x_n，$\cdots$，x 的n个线性型，其系数行列式为Δ，则有一异于原点的整点$(x_1, \cdots, x_n)$，使

$$|\xi_1|+\cdots+|\xi_n|\leqslant(n!|\Delta|)^{\frac{1}{n}}.$$

定理9 有一异于原点的整点，使

$$|\xi_1\cdots\xi_n|\leqslant\frac{n!}{n^n}|\Delta|.$$

定理10 若$a_1, \cdots, a_n$ 是 n 个实数，则有一异于原点的整点$(x_1, \cdots, x_n)$及整数 $y\geqslant 1$，使

$$\left|a_i-\frac{x_i}{y}\right|\leqslant\frac{n}{(n+1)y^{1+\frac{1}{n}}}, \quad i=1, 2, \cdots, n.$$

定理11 若$\alpha+\beta=1$，$\alpha>0$，$\beta>0$，则对$s\geqslant 0$，$t\geqslant 0$，恒有

$$s^{\alpha}t^{\beta}\leqslant s\alpha+t\beta,$$

且等号只当$s=t$时成立。

定理12 若$\alpha+\beta=1$，$\alpha>0$，$\beta>0$，则当a与b不成比例时，恒有

$$\sum_{i=1}^{n}a_i^{\alpha}b_i^{\beta}<\left(\sum_{i=1}^{n}a_i\right)^{\alpha}\left(\sum_{i=1}^{n}b_i\right)^{\beta}.$$

定理13 命$n\geqslant 2$，ξ_1，…，ξ_n是x_1，…，x_n的n个线性型，其系数行列式$\Delta\neq 0$；其中有s对型是有共轭复数系数的，有r个型是实系数的，$r+2s=n$。若$\sigma\geqslant 1$，则有一异于原点的整点，使

$$\left(\frac{|\xi_1|^{\sigma}+\cdots+|\xi_n|^{\sigma}}{n}\right)^{\frac{1}{\sigma}}\leqslant\left(\frac{\left(\frac{2}{\pi}\right)^{s}n^{-\frac{n}{\sigma}}\Gamma\left(1+\frac{n}{\sigma}\right)|\Delta|}{2^{-\frac{2s}{\sigma}}\Gamma^{r}\left(1+\frac{1}{\sigma}\right)\Gamma^{s}\left(1+\frac{2}{\sigma}\right)}\right)^{\frac{1}{n}}.$$

定理14 与定理13的假定相同。若λ_1，…，λ_n是n个正数，$\lambda_{r+t}=\lambda_{r+s+t}$（$t=1$，…，$s$）及

$$\lambda_1\cdots\lambda_{r+2s}\geqslant\left(\frac{2}{\pi}\right)^{s}|\Delta|,$$

则必有一异于原点的整点，使

$$|\xi_1|\leqslant\lambda_1,\ \cdots,\ |\xi_n|\leqslant\lambda_n.$$

定理15 与定理13的假定相同。命

$$\xi_{\nu}=\eta_{\nu}\ (1\leqslant\nu\leqslant r),$$

$$\xi_{r+\nu}=\eta_{r+\nu}+i\eta_{r+s+\nu},\ \xi_{r+s+\nu}=\bar{\xi}_{r+\nu},\ (1\leqslant\nu\leqslant s).$$

若$\lambda_1\cdots\lambda_n\geqslant\frac{|\Delta|}{2^s}$，则有一异于原点的整点，使

$$|\eta_{\nu}|\leqslant\lambda_{\nu}\ (1\leqslant\nu\leqslant n).$$

定理16 当x_1，…，x_n取整数时，命m为

$$|(\xi_1-\rho_1)\cdots(\xi_n-\rho_n)|$$

的下界，则

$$m\leqslant 2^{-\frac{n}{2}}|\Delta|,$$

其中ξ_1，…，ξ_n；ρ_1，…，ρ_n均为实数；ξ_1，…，ξ_n是x_1，…，x_n的n个线性型且Δ是系数行列式。

定理17 仅在有理数域内，基数$\Delta=1$。

定理18 若Δ为一有理整数，则必有一有限数$n(\Delta)$，使凡基数为Δ的代数数域的次数均不大于$n(\Delta)$。

定理19 对于固定的有理整数Δ，至多只有有限个代数数域以Δ为基数。

定理20 命$R(\theta)$为一n次代数数域。如果$\theta^{(1)}$，$\theta^{(n)}$中有r_1个实数，r_2对共轭复数，$r_1+2r_2=n$，那么$R(\theta)$的基数Δ适合

$$|\Delta|\geqslant\left(\frac{\pi}{4}\right)^{2r_2}\left(\frac{n^n}{n!}\right)^2.$$

二、题 解

§ 联立渐近法

习题 若$\alpha_\nu=\beta_\nu+i\gamma_\nu(\nu=1, 2\cdots, n)$是$n$个复数，则有复整数$z_1$，…，$z_n$，$\omega$存在，使

$$\left|\alpha_\nu-\frac{z_\nu}{\omega}\right|\leqslant\frac{n}{n+1}\cdot\frac{2}{\sqrt{\pi}}\left(\frac{2n+1}{n+1}\cdot\frac{4}{\pi}\right)^{\frac{1}{2n}}\frac{1}{|\omega|^{1+\frac{1}{n}}}.$$

证：设 $z_\nu=x_\nu+iy_\nu$，　$\nu=1, 2, \cdots n$，

$$\omega=a+ib.$$

不失一般，可设$n\geqslant 2$。要使

$$\left| a_v - \frac{z_v}{\omega} \right| \leqslant \frac{n}{n+1} \cdot \sqrt{\frac{2}{\pi}} \left(\frac{2n+1}{n+1} \cdot \frac{4}{\pi} \right)^{\frac{1}{2n}} \frac{1}{|\omega|^{1+\frac{1}{n}}}$$

由于 $\left|a_v - \frac{z_v}{\omega}\right| = \left| \beta_v + i\gamma_v - \frac{x_v + iy_v}{a+ib} \right|$

$$= \left| \beta_v + i\gamma_v - \frac{(x_v + iy_v)(a-ib)}{a^2+b^2} \right|$$

$$= \left| \left(\beta_v - \frac{ax_v + by_v}{a^2+b^2}\right) + i\left(\gamma_v - \frac{ay_v - bx_v}{a^2+b^2}\right) \right|$$

$$= \left| \frac{(a^2+b^2)\beta_v - (ax_v + by_v)}{a^2+b^2} + i\, \frac{(a^2+b^2)\gamma_v - (ay_v - bx_v)}{a^2+b^2} \right|$$

$$= \sqrt{\left(\frac{(ax_v + by_v) - (a^2+b^2)\beta_v}{a^2+b^2} \right)^2 + \left(\frac{(ay_v - bx_v) - (a^2+b^2)\gamma_v}{a^2+b^2} \right)^2}$$

因此只需

$$\Big((ax_v + by_v) - (a^2+b^2)\beta_v \Big)^2 + \Big((ay_v - bx_v) - (a^2+b^2)\gamma_v \Big)^2$$

$$\leqslant \left(\frac{n}{n+1} \right)^2 \cdot \frac{4}{\pi} \cdot \left(\frac{2n+1}{n+1} \cdot \frac{4}{\pi} \right)^{\frac{1}{n}} \Big((a^2+b^2) \Big)^{1-\frac{1}{n}}.$$

又因为 $\Big((ax_v + by_v) - (a^2+b^2)\beta_v \Big)^2 + \Big((ay_v - bx_v) -$

$$(a^2+b^2)\gamma_v \Big)^2 = (a^2+b^2)x_v^2 + (a^2+b^2)y_v^2 -$$

$$2(a^2+b^2)(a\beta_v - b\gamma_v)x_v - 2(a^2+b^2)(b\beta_v + a\gamma_v)y_v +$$

$$(a^2+b^2)^2(\beta_v^2 + \gamma_v^2),$$

并且 $(a\beta_v - b\gamma_v)^2 + (b\beta_v + a\gamma_v)^2 = (a^2+b^2)(\beta_v^2 + \gamma_v^2)$

故只需 $\Big(x_v - (a\beta_v - b\gamma_v) \Big)^2 + \Big(y_v - (b\beta_v + a\gamma_v) \Big)^2 \leqslant$

$$\left(\frac{n}{n+1} \right)^2 \cdot \frac{4}{\pi} \cdot \left(\frac{2n+1}{n+1} \cdot \frac{4}{\pi} \right)^{\frac{1}{n}} (a^2+b^2)^{-\frac{1}{n}} \qquad (1)$$

即可。

取$\omega=i$即取$a=0$，$b=1$，则(1)式给出

$$(x_v+\gamma_v)^2+(y_v-\beta_v)^2\leqslant\left(\frac{n}{n+1}\right)^2\cdot\frac{4}{\pi}\cdot\left(\frac{2n+1}{n+1}\cdot\frac{4}{\pi}\right)^{\frac{1}{n}} \quad (2)$$

又当$n\geqslant 2$时，显然有

$$\left(\frac{n}{n+1}\right)^2\cdot\frac{4}{\pi}\cdot\left(\frac{2n+1}{n+1}\cdot\frac{4}{\pi}\right)^{\frac{1}{n}}>\frac{16}{9\pi}>\frac{1}{2} \quad (3)$$

i） 如果$\{\gamma_v\}\leqslant\frac{1}{2}$，$\{\beta_v\}\leqslant\frac{1}{2}$，则取

$x_v=-[\gamma_v]$，$y_v=[\beta_v]$；

ii） 如果$\{\gamma_v\}\leqslant\frac{1}{2}$，$\{\beta_v\}>\frac{1}{2}$，则取

$x_v=-[\gamma_v]$，$y_v=[\beta_v]-1$；

iii） 如果$\{\gamma_v\}>\frac{1}{2}$，$\{\beta_v\}\leqslant\frac{1}{2}$，则取

$x_v=-\left([\gamma_v]+1\right)$，$y_v=[\beta_v]$；

Ⅳ） 如果$\{\gamma_v\}>\frac{1}{2}$，$\{\beta_v\}>\frac{1}{2}$，则取

$x_v=-\left([\gamma_v]+1\right)$，$y_v=[\beta_v]-1$。

以上四种情形均给出

$$(x_v+\gamma_v)^2+(y_v-\beta_v)^2<\frac{1}{2} \quad (4)$$

由（2）、（3）、（4）可知，（1）式对于有理整数x_v、y_v、a、b的确有解，即对于任意给定的n个复数

$a_v=\beta_v+i\beta$，$v=1, 2, \cdots\cdots, n$

的确可以找到复整数$z_1\cdots$，z，ω，使得不等式

$$\left|a_v-\frac{z}{\omega}\right|\leqslant\frac{n}{n+1}\cdot\frac{2}{\sqrt{\pi}}\cdot\left(\frac{2n+1}{n+1}\cdot\frac{4}{\pi}\right)^{\frac{1}{2n}}\frac{1}{|\omega|^{1+\frac{1}{n}}}$$

成立。

§10 在代数数论上的应用

习题1 证明在一理想数Q中可以选得一整数α，使

$$|N(\alpha)|\leqslant\sqrt{|\Delta|}N(Q)。$$

证： 用$R(\theta)$表一n次代数数域，$\omega_1\cdots$，ω_n是$R(\theta)$的一组整底；设Q为$R(\theta)$上的一个理想数，$\alpha_1\cdots$，α_n是Q的一组基底；再用Δ、$\Delta(Q)$分别表$R(\theta)$、Q的基数和判别式。

下面首先利用本节的一个等式

$$(x_1\omega_1+\cdots x_n\omega_n)^{(i)}=x_1\omega_1^{(i)}+\cdots+x_n\omega_n^{(i)},\quad 1\leqslant i\leqslant n$$

来证明：

若 $\quad \alpha=x_1\alpha_1+x_2\alpha_2+\cdots+x_n\alpha_n \qquad (1)$

则 $\quad \alpha^{(i)}=x_1\alpha_1^{(i)}+x_2\alpha_2^{(i)}+\cdots x_n\alpha_n^{(i)},\quad 1\leqslant i\leqslant n。$

因为ω_1，…，ω_n是$R(\theta)$的一组整底，所以存在有理整数a_{rs}（$1\leqslant r\leqslant n$，$1\leqslant s\leqslant n$），使得下面诸等式成立：

$$\alpha_1=a_{11}\omega_1+a_{12}\omega_2+\cdots+a_{1n}\omega_n$$
$$\alpha_2=a_{21}\omega_1+a_{22}\omega_2+\cdots+a_{2n}\omega_n \qquad (2)$$
$$\cdots\cdots$$
$$\alpha_n=a_{n1}\omega_1+a_{n2}\omega_2+\cdots+a_{nn}\omega_n$$

由（2）得

$$\alpha_1^{(i)}=a_{11}\omega_1^{(i)}+a_{12}\omega_2^{(i)}+\cdots+a_{1n}\omega_n^{(i)}$$
$$\alpha_2^{(i)}=a_{21}\omega_1^{(i)}+a_{22}\omega_2^{(i)}+\cdots+a_{2n}\omega_n^{(i)} \qquad (3)$$
$$\cdots\cdots$$

$$\alpha_n^{(i)}=a_{n1}\omega_1^{(i)}+a_{n2}\omega_2^{(i)}+\cdots+a_{nn}\omega_n^{(i)}$$

由（3）得 $x_1\alpha_1^{(i)}+x_2\alpha_2^{(i)}+\cdots+x_n\alpha_n^{(i)}=(x_1a_{11}+x_2a_{21}+\cdots+x_na_{n1})\omega_1^{(i)}+(x_1a_{12}+x_2a_{22}+\cdots+x_na_{n2})\omega_2^{(i)}+\cdots+(x_1a_{1n}+x_2a_{2n}+\cdots+x_na_{nn})\omega_n^{(i)}$ （4）

把（2）代入（1）得

$$\begin{aligned}\alpha&=x_1\alpha_1+x_2\alpha_2+\cdots+x_n\alpha_{n}\\&=(x_1a_{11}+x_2a_{21}+\cdots+x_na_{n1})\omega_1+(x_1a_{12}+x_2a_{22}+\cdots\\&\quad+x_na_{n2})\omega_2+\cdots\cdots\\&\quad+(x_1a_{1n}+x_2a_{2n}+\cdots+x_na_{nn})\omega_n,\end{aligned}$$

所以

$$\begin{aligned}\alpha^{(i)}&=(x_1a_{11}+x_2a_{21}+\cdots+x_na_{n1})\omega_1^{(i)}+(x_1a_{12}+x_2a_{22}\\&\quad+\cdots+x_na_{n2})\omega_2^{(i)}+\cdots\\&\quad+(x_1a_{1n}+x_2a_{2n}+\cdots+x_na_{nn})\omega_n^{(i)}\end{aligned}\qquad(5)$$

从（4）和（5）立得

$$\alpha^{(i)}=x_1\alpha_1^{(i)}+x_2\alpha_2^{(i)}+\cdots+x_n\alpha_n^{(i)},\quad 1\leqslant i\leqslant n.$$

又因为第16章第9节定理2给出

$$\Delta(\mathbf{Q})=N(\mathbf{Q})^2\Delta$$

$$\sqrt{|\Delta(\mathbf{Q})|}=\sqrt{|\Delta|}\,N(\mathbf{Q})$$

因此，方程组

$$\alpha^{(i)}=x_1\alpha_1^{(i)}+x_2\alpha_2^{(i)}+\cdots+x_n\alpha_n^{(i)},\quad 1\leqslant i\leqslant n$$

的系数行列式的绝对值等于

$$\sqrt{|\Delta(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)|}=\sqrt{|\Delta(\mathbf{Q})|}=\sqrt{|\Delta|}\,N(\mathbf{Q}).$$

如果取

$$\lambda_1=\lambda_2=\cdots=\lambda_{n-1}=\frac{1}{2},\qquad \lambda=2^{n-1}\sqrt{|\Delta|}\,N(\mathbf{Q})$$

那么由提要中定理15知道有一组不全为零的整数x_1，x_2，…，x_n，使得

$$|\alpha| = |\alpha^{(1)}| \leqslant \frac{1}{2}, \quad |\alpha^{(2)}| \leqslant \frac{1}{2}, \quad \cdots, \quad |\alpha^{(n-1)}| \leqslant \frac{1}{2},$$

$$|\alpha^{(n)}| \leqslant 2^{n-1}\sqrt{|\Delta|}\,N(\mathbf{Q}).$$

故若取$\alpha = \alpha^{(1)}$，则由

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$

的α_1，α_2，…，α_n为Q的基底知道$\alpha \in \mathbf{Q}$。此时有

$$|N(\alpha)| = |\alpha^{(1)}|\,|\alpha^{(2)}|\cdots|\alpha^{(n)}| \leqslant \sqrt{|\Delta|}\,N(\mathbf{Q}).$$

即在一理想Q中，可以选得一整数α，使$|N(\alpha)| \leqslant \sqrt{|\Delta|}\,N(\mathbf{Q})$成立。

习题 2 证明任一理想数类中有一理想数Q适合于

$$N(\mathbf{Q}) \leqslant \sqrt{|\Delta|}.$$

证：设h为$R(\theta)$上理想数类的类数，Δ为$R(\theta)$的基数；再用$\mathbf{A}_1$，$\mathbf{A}_2$，…$\mathbf{A}_h$表不同的理想数类，

由习题 1 可知，对任一理想数$\mathbf{A}_i$（$1 \leqslant i \leqslant h$），均存在整数$\alpha_i \in \mathbf{A}_i$（$1 \leqslant i \leqslant h$），使得

$$\frac{|N(\alpha_i)|}{N(\mathbf{A}_i)} \leqslant \sqrt{|\Delta|}, \quad (1 \leqslant i \leqslant h).$$

因为$\alpha_i \in \mathbf{A}_i$，从而$\mathbf{A}_i \mid [\alpha_i]$，故可设

$$[\alpha_i] = \mathbf{A}_i\mathbf{B}_i, \quad (1 \leqslant i \leqslant h).$$

由 $$|N(\alpha_i)| = N(\mathbf{A}_i)N(\mathbf{B}_i)$$

和 $$\frac{|N(\alpha_i)|}{N(\mathbf{A}_i)} \leqslant \sqrt{|\Delta|}$$

可得 $$N(\mathbf{B}_i) \leqslant \sqrt{|\Delta|}, \quad (1 \leqslant i \leqslant h).$$

因此只需再证明：对任意的i、j（$i \neq j$，$1 \leqslant i$，$j \leqslant h$）$\mathbf{B}_i$与$\mathbf{B}_j$决不相似，则本题结论就被证明了。

因为 $$[\alpha_i] = \mathbf{A}_i\mathbf{B}_i, \quad [\alpha_j] = \mathbf{A}_j\mathbf{B}_j$$

所以 $$\mathbf{A}_i\mathbf{B}_i \sim \mathbf{A}_j\mathbf{B}_j$$

如果$\mathbf{B}_i \sim \mathbf{B}_j$，则易证$\mathbf{A}_i \sim \mathbf{A}_j$，此与假设矛盾，故$\mathbf{B}_i$与$\mathbf{B}_j$决不能相

似，此即

$$\mathbf{B}_1, \ \mathbf{B}_2, \ \cdots \mathbf{B}_h$$

也代表不同的理想数类，如果取Q＝B，那么Q就适合

$$N(\mathrm{Q}) \leqslant \sqrt{|\Delta|}$$

而i可取1，2…，h诸数，因此任一理想数类中必有一理想数Q存在，使得$N(\mathrm{Q}) \leqslant \sqrt{|\Delta|}$成立。

参考文献

〔1〕华罗庚　高等数学引论　科学出版社　1979年版

〔2〕华罗庚　堆垒素数论　科学出版社　1962年版

〔3〕闵嗣鹤　数论的方法　科学出版社　1983年版

〔4〕N.M.维诺格拉陀夫著　裘光明译　数论基础　高等教育出版社　1956年版

〔5〕柯召、孙琦　谈谈不定方程　上海教育出版社　1980年版

〔6〕陈景润　初等数论　科学出版社　1978年版

〔7〕潘承洞　素数分布与哥德巴赫猜想　山东科学技术出版社　1979年版

〔8〕王元　谈谈素数　上海教育出版社　1983年版

〔9〕G.H. HARDY AND E.M.WRIGHT AN INTRODUCTION TO THE THEORY OF NUMBERS OXFORD UNIVERSITY PRESS 1981年版

〔10〕L.J. Mordell, Diophantine Equations, Academic, 1969年版

〔11〕Tom M. Apostol, Introduction to analytic number theory.New York, Springer, 1976年版

〔12〕Tom M. Apostol, Modular Functions and Dirichlet Series in Number Theory. New York, Springer, 1976年版

编　后

数论是探究整数性质的一门学科．在这块“数学王国”的领地上，我国不少数学家都曾辛勤耕耘．而在用以记载并传播他们丰硕成果的众多著述中，首屈一指的，则无疑要推已故华罗庚教授的《数论导引》了．

似乎很难置信，象任承俊这样一个一九八一年才从大学毕业的年青人，现在就能够做出《数论导引》的全部习题，而且能够指出并订正其疏漏之处．然而读罢书稿，疑团消散了．随之纷沓而来的有喜悦，有慰藉，有赞佩，也有“后生可畏”的感慨．

透过《数论导引提要及习题解答》，我们可以窥见，一代年轻的探索者，正踏着华罗庚教授的足迹，朝着通向“数学王国”的荆棘之路闯去；同时还会感到，他们那急骤的脚步声，撞击着我们的心灵，鞭策着我们奋进．至于本书的水平与价值究竟如何，这里存而不论，留待诸位读者去评说吧！

编余废墨，谬充后记．

编　者

一九八五年六月二十九日

［Ｇｅｎｅｒａｌ Ｉｎｆｏｒｍａｔｉｏｎ］
书名＝数论导引提要及习题解答
作者＝任承俊编著
页数＝４８７
ＳＳ号＝１０５２８３０３
出版日期＝１９８６年０９月第１版